E ผช.ทส.19/2568

สบอ 11298/21 ส.ค. 68

ผส.บอ.8360

บันทึกข้อความ

ส่วนราชการ คณะทำงานขับเคลื่อนแผนปฏิบัติการการรักษาความมั่นคงทางไซเบอร์ กรมชลประทาน โทร. ๒๙๖๖

ที่ ศทส. ๓๔๙๖ /๒๕๖๘ **วันที่** ๒๑ สิงหาคม ๒๕๖๘

เรื่อง ขอแจ้งเตือนเหตุที่อาจก่อให้เกิดภัยคุกคามทางไซเบอร์

เรียน ผู้อำนวยการสำนัก กอง ศูนย์ กลุ่ม และสถาบัน

ตามที่คณะทำงานขับเคลื่อนแผนปฏิบัติการการรักษาความมั่นคงทางไซเบอร์ กรมชลประทาน ซึ่งปฏิบัติงานเป็นหน่วยงานควบคุมและกำกับดูแล (Regulator) และกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ในสังกัด ได้รับแจ้งจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช) กรณีเกิดช่องโหว่ทางไซเบอร์ ทำให้ผู้โจมตีจากระยะไกลสามารถใช้โค้ดอันตรายเข้าถึงไฟล์สำคัญในระบบได้ และรันคำสั่งบนระบบได้โดยตรง นั้น

เพื่อเป็นการป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาต รวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน คณะทำงานขับเคลื่อนแผนปฏิบัติการการรักษาความมั่นคงทางไซเบอร์ กรมชลประทาน จึงขอแจ้งเตือนเหตุที่อาจก่อให้เกิดภัยคุกคามดังกล่าว และแนวทางการป้องกัน รายละเอียดตามเอกสารที่แนบ

จึงเรียนมาเพื่อโปรดทราบ

(นายธนพล สงวนตระกูล)
ผอ.ทส.
เลขานุการคณะทำงานขับเคลื่อนฯ

เรียน ผอ.ส่วน ผอช.ภาค ทน. ๑ - ๙ บอ. และหัวหน้าฝ่ายในส่วนบริหารทั่วไป
เพื่อทราบ

(นายธเนศร์ สมบูรณ์)
ผส.บอ. 66 ส.ค. 68

TLP:CLEAR

เอกสารการแจ้งเตือนกรณีช่องโหว่ระดับ Critical ในผลิตภัณฑ์ Endpoint Security Products ของ Trend Micro

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีช่องโหว่ระดับ Critical ในผลิตภัณฑ์ Endpoint Security Products ของ Trend Micro[1]

Trend Micro ได้ออกประกาศเปิดตัวเครื่องมือแก้ไขชั่วคราว (FixTool) เพื่อลดความเสี่ยงจากช่องโหว่ในผลิตภัณฑ์ป้องกันปลายทาง Endpoint Security Products พร้อมแนะนำให้ผู้ใช้และผู้ดูแลระบบนำไปใช้ทันที เพื่อป้องกันการถูกโจมตี โดยช่องโหว่ที่ระบุได้แก่ CVE-2025-54948[2] และ CVE-2025-54987[3] (มีคะแนน CVSS : 9.4) โดยเป็นช่องโหว่ประเภท command injection ที่ทำให้ผู้โจมตีจากระยะไกลสามารถใช้เพื่ออัปโหลดโค้ดอันตรายและรันคำสั่งบนระบบได้ โดยไม่จำเป็นต้องผ่านการยืนยันตัวตน (Pre-authenticated Remote Code Execution)

ผลิตภัณฑ์ที่ได้รับผลกระทบ

- Trend Micro Apex One (on-premise)
- Trend Micro Apex One as a Service
- Trend Vision One Endpoint Security – Standard Endpoint Protection

แนวทางการป้องกัน

- ผู้ใช้และผู้ดูแลระบบ Apex One (On-premise) ควรติดตั้ง FixTool ทันทีเป็นมาตรการป้องกันชั่วคราว ในขณะที่ Trend Micro จะปล่อยแพตช์ความปลอดภัยฉบับสมบูรณ์ต่อไป[4]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-077
2. https://nvd.nist.gov/vuln/detail/CVE-2025-54948
3. https://nvd.nist.gov/vuln/detail/CVE-2025-54987
4. https://success.trendmicro.com/en-US/solution/KA-0020652

TLP:CLEAR

TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Microsoft ได้ออกแพตช์ความปลอดภัยเพื่อแก้ไขช่องโหว่ในซอฟต์แวร์และผลิตภัณฑ์-

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์กรณี Microsoft ได้ออกแพตช์ความปลอดภัย เพื่อแก้ไขช่องโหว่ในซอฟต์แวร์และผลิตภัณฑ์[1]

Microsoft ได้ออกแพตช์ความปลอดภัยประจำเดือนสิงหาคม 2025 เพื่อแก้ไขช่องโหว่ในซอฟต์แวร์และผลิตภัณฑ์ โดยมีช่องโหว่ที่สำคัญจำนวน 17 รายการ ที่เสี่ยงต่อการถูกโจมตีจากระยะไกล (Remote Code Execution) หรือการยกระดับสิทธิ์ (Elevation of Privilege) ที่อาจทำให้ผู้โจมตีใช้ประโยชน์จากช่องโหว่เหล่านี้ในการเข้าถึงหรือควบคุมระบบได้ **โดยมีรายละเอียดตามเอกสารแนบ**

<u>ผลกระทบ</u>

- ผู้โจมตีสามารถยกระดับสิทธิ์การเข้าถึงจากระดับผู้ใช้ทั่วไปเป็นระดับผู้ดูแลหรือเข้าถึงข้อมูลได้
- ผู้โจมตีสามารถใช้รันโค้ดอันตรายบนเครื่องเป้าหมายจากระยะไกลได้
- ผู้โจมตีที่มีบัญชีผู้ใช้ระดับต่ำบน Azure Portal สามารถยกระดับสิทธิ์ขึ้นเป็นผู้ดูแลระบบได้
- ผู้โจมตีใช้ช่องโหว่ในโปรโตคอล NTLM เพื่อดักจับหรือปลอมแปลงข้อมูลยืนยันตัวตนและเพิ่มสิทธิ์การเข้าถึง

<u>แนวทางการป้องกัน</u>

- อัปเดตแพตช์ผ่าน Windows Update, WSUS หรือ Microsoft Endpoint Manager
- จัดลำดับความสำคัญให้กับระบบที่เกี่ยวข้องกับ Azure, Windows Graphics, GDI+, Microsoft Office/Word และ NTLM
- เปิดใช้งานการป้องกันเสริม เช่น การบล็อก Office Macro, ใช้งานระบบ IDS/IPS และตรวจสอบความผิดปกติของ Log

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-079/

เอกสารแนบรายละเอียดของช่องโหว่

CVE Number	ชื่อช่องโหว่	คะแนน CVSS	รายละเอียดเพิ่มเติม
CVE-2025-53767	Azure OpenAI Elevation of Privilege Vulnerability	10.0	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53767
CVE-2025-50165	Windows Graphics Component Remote Code Execution Vulnerability	9.8	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-50165
CVE-2025-53766	GDI+ Remote Code Execution Vulnerability	9.8	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53766
CVE-2025-53792	Azure Portal Elevation of Privilege Vulnerability	9.1	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53792
CVE-2025-53778	Windows NTLM Elevation of Privilege Vulnerability	8.8	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53778
CVE-2025-53784	Microsoft Word Remote Code Execution Vulnerability	8.4	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53784
CVE-2025-53733	Microsoft Word Remote Code Execution Vulnerability	8.4	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53733
CVE-2025-53740	Microsoft Office Remote Code Execution Vulnerability	8.4	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53740
CVE-2025-53731	Microsoft Office Remote Code Execution Vulnerability	8.4	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53731
CVE-2025-53787	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	8.2	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53787
CVE-2025-50177	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	8.1	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-50177

CVE Number	ชื่อช่องโหว่	คะแนน CVSS	รายละเอียดเพิ่มเติม
CVE-2025-49707	Azure Virtual Machines Spoofing Vulnerability	7.9	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-49707
CVE-2025-50176	DirectX Graphics Kernel Remote Code Execution Vulnerability	7.8	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-50176
CVE-2025-53781	Azure Virtual Machines Information Disclosure Vulnerability	7.7	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53781
CVE-2025-48807	Windows Hyper-V Remote Code Execution Vulnerability	7.5	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-48807
CVE-2025-53793	Azure Stack Hub Information Disclosure Vulnerability	7.5	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53793
CVE-2025-53774	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	6.5	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2025-53774

TLP:CLEAR

เอกสารการแจ้งเตือนกรณี ช่องโหว่ Zero-Day ระดับ Critical ใน Adobe Experience Manager

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์กรณี ช่องโหว่ Zero-Day ระดับ Critical ใน Adobe Experience Manager[1]

Adobe ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ Zero-Day ระดับ Critical ใน Adobe Experience Manager (AEM) Forms บน Java Enterprise Edition (JEE) หลังจากมีการเผยแพร่โค้ดตัวอย่างการโจมตี (PoC) ซึ่งสามารถนำไปใช้รันคำสั่งบนเซิร์ฟเวอร์ที่มีช่องโหว่ได้

รายละเอียดช่องโหว่

- CVE-2025-54253[2] (คะแนน CVSS: 10) เป็นช่องโหว่ที่เกิดจากการตั้งค่าผิดพลาด (Misconfiguration) ทำให้ผู้โจมตีสามารถรันโค้ดจากระยะไกล (Remote Code Execution) บนระบบได้โดยตรง และอาจขยายการเข้าถึงเพื่อโจมตีส่วนอื่นของระบบ
- CVE-2025-54254[3] (คะแนน CVSS: 8.6) เป็นช่องโหว่ประเภท Improper Restriction of XML External Entity Reference (XXE) ทำให้ผู้โจมตีสามารถเข้าถึงไฟล์สำคัญในระบบได้ โดยไม่ต้องมีการโต้ตอบจากผู้ใช้งาน ส่งผลให้ข้อมูลลับหรือข้อมูลสำคัญเสี่ยงต่อการรั่วไหล

ผลิตภัณฑ์ที่ได้รับผลกระทบ

- AEM Forms บน JEE เวอร์ชัน 6.5.23 และเวอร์ชันก่อนหน้า

แนวทางการป้องกัน

แนะนำให้อัปเดตแพตช์ล่าสุดที่ Adobe เผยแพร่เพื่อแก้ไขช่องโหว่[4] หากไม่สามารถอัปเดตได้ทันที ควรดำเนินการลดความเสี่ยง ดังนี้

- จำกัดการเข้าถึง AEM Forms จากเครือข่ายภายนอก
- กำหนดสิทธิ์ผู้ใช้งานและแอปพลิเคชันให้น้อยที่สุดเท่าที่จำเป็น (Least Privilege)

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-078
2. https://nvd.nist.gov/vuln/detail/CVE-2025-54253
3. https://nvd.nist.gov/vuln/detail/CVE-2025-54254
4. https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

TLP:CLEAR

TLP:CLEAR

เอกสารการแจ้งเตือนกรณีช่องโหว่ FortiSIEM (CVE-2025-25256)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีช่องโหว่ FortiSIEM (CVE-2025-25256)[1]

Fortinet ได้ออกแพตช์ความปลอดภัยเพื่อแก้ไขช่องโหว่ระดับ Critical ในผลิตภัณฑ์ FortiSIEM ที่หมายเลข CVE-2025-25256[2] มีคะแนนความรุนแรง CVSS : 9.8 โดยเป็นช่องโหว่ประเภท OS Command Injection ทำให้ผู้โจมตีที่ไม่ได้ยืนยันตัวตน (Unauthenticated) สามารถรันคำสั่งหรือโค้ดที่ไม่ได้รับอนุญาตผ่านคำสั่ง Command-Line Interface (CLI) ที่ถูกสร้างขึ้นมาได้[3]

เวอร์ชันที่ได้รับผลกระทบ

- FortiSIEM 6.1, 6.2, 6.3, 6.4, 6.5, 6.6
- FortiSIEM 6.7.0 - 6.7.9
- FortiSIEM 7.0.0 - 7.0.3
- FortiSIEM 7.1.0 - 7.1.7
- FortiSIEM 7.2.0 - 7.2.5
- FortiSIEM 7.3.0 - 7.3.1

แนวทางการป้องกันและลดผลกระทบ

- อัปเดตแพตช์เวอร์ชันล่าสุดที่ Fortinet ได้ออกแก้ไขแล้ว
- หากไม่สามารถอัปเดตได้ทันที ให้จำกัดการเข้าถึงพอร์ต phMonitor (7900) เพื่อปิดช่องทางการโจมตี

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-080
2. https://nvd.nist.gov/vuln/detail/CVE-2025-25256
3. https://thehackernews.com/2025/08/fortinet-warns-about-fortisiem.html

เอกสารการแจ้งเตือนกรณีช่องโหว่ Firewall Management Center ของ Cisco

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์กรณีช่องโหว่ Firewall Management Center ของ Cisco[1]

Cisco ได้ออกแจ้งเตือนเกี่ยวกับช่องโหว่ระดับ Critical ที่หมายเลข CVE-2025-20265[2] มีคะแนนความรุนแรง CVSS : 10.0 ที่ส่งผลกระทบต่อซอฟต์แวร์ Secure Firewall Management Center (FMC) ซึ่งช่องโหว่ดังกล่าวอยู่ใน RADIUS Subsystem ที่ใช้สำหรับการยืนยันตัวตนเพื่อควบคุมการเข้าถึงระบบแบบรวมศูนย์ ความบกพร่องดังกล่าวเกิดจากการตรวจสอบและจัดการข้อมูลนำเข้า (user input) ที่ไม่ถูกต้องในขั้นตอนการยืนยันตัวตน ทำให้ผู้โจมตีสามารถส่งข้อมูลที่ถูกสร้างขึ้นเป็นพิเศษ (specially crafted input) ระหว่างการล็อกอินผ่าน RADIUS Authentication และนำไปสู่การรันคำสั่งใน Shell ได้โดยไม่ต้องยืนยันตัวตน (Remote Code Execution – RCE) พร้อมสิทธิ์ระดับสูงได้

<u>เวอร์ชันที่ได้รับผลกระทบ</u> : FMC เวอร์ชัน 7.0.7 และ 7.7.0 (เมื่อเปิดใช้งาน RADIUS บน web interface หรือ SSH management)

<u>แนวทางการป้องกันและลดผลกระทบ</u>

- ผู้ใช้งานควรอัปเดตซอฟต์แวร์ที่ Cisco ได้ออกแก้ไขแล้ว
- หากไม่สามารถติดตั้งแพตช์ได้ ให้ปิดการใช้งาน RADIUS Authentication และใช้วิธีอื่นแทน เช่น Local account, LDAP หรือ SAML SSO

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.bleepingcomputer.com/news/security/cisco-warns-of-max-severity-flaw-in-firewall-management-center/
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79