แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Microsoft, Cisco, Fortinet และ NGINX ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์

วันที่แจ้งเตือน 15 พฤษภาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Microsoft, Cisco, Fortinet และ NginX ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ ดังนี้

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	• ช่องโหว่ CVE-2026-40361 เกี่ยวข้องกับการประมวลผลอีเมลภายใน Outlook โดยระบบจะประมวลผลเนื้อหาหรือองค์ประกอบของอีเมลโดยอัตโนมัติเมื่ออีเมลถูกส่งถึง Inbox หรือการประมวลผลผ่าน Preview Pane ทำให้ผู้ไม่หวังดีสามารถรันโค้ดอันตรายจากระยะไกล (Remote Code Execution: RCE) ได้โดยที่ผู้ใช้งานไม่จำเป็นต้องเปิดอีเมลหรือคลิกลิงก์ (Zero-Click Outlook Vulnerability)	Microsoft Outlook บางเวอร์ชันที่ใช้งานบนระบบ Microsoft Windows รวมถึงระบบที่เชื่อมต่อกับ Microsoft Exchange
Cisco	• ช่องโหว่ CVE-2026-20182 เกิดจากข้อบกพร่องของขั้นตอนการยืนยันตัวตน (Authentication Bypass) ในระบบ Cisco Catalyst SD-WAN Controller และ Cisco Catalyst SD-WAN Manager ทำให้ผู้ไม่หวังดีสามารถส่ง HTTP Request ที่สร้างขึ้นเข้าสู่ระบบ เพื่อเข้าถึงหรือเรียกใช้ API ได้จากระยะไกลโดยไม่ต้องยืนยันตัวตน ซึ่งกำลังใช้โจมตีจริงในลักษณะ Zero-Day	Cisco Catalyst SD-WAN Manager • On-Prem Deployment • Cisco SD-WAN Cloud-Pro • Cisco SD-WAN Cloud (Cisco Managed) • Cisco SD-WAN for Government (FedRAMP)

ข้อมูลอ้างอิง Microsoft

1. https://www.securityweek.com/microsoft-patches-critical-zero-click-outlook-vulnerability-threatening-enterprises/
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361
3. https://nvd.nist.gov/vuln/detail/CVE-2026-40361

ข้อมูลอ้างอิง Cisco

1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
2. https://nvd.nist.gov/vuln/detail/CVE-2026-20182
3. https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-critical-sd-wan-flaw-exploited-in-zero-day-attacks/
4. https://thehackernews.com/2026/05/cisco-catalyst-sd-wan-controller-auth.html

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Microsoft, Cisco, Fortinet และ NGINX ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์

วันที่แจ้งเตือน 15 พฤษภาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Fortinet	• ช่องโหว่ CVE-2026-26083 เกิดจาก Missing Authorization ที่อนุญาตให้ผู้โจมตีที่ไม่ได้ยืนยันตัวตนสามารถส่งคำขอ HTTP เพื่อสั่งรันโค้ดหรือคำสั่งอันตราย (RCE) ได้	FortiSandbox 4.4, 5.0 และ FortiSandbox Cloud 23, 24
	• ช่องโหว่ CVE-2026-44277 เกิดจากการควบคุมและจัดการสิทธิการเข้าถึงที่ไม่เหมาะสม (Improper Access Control) ทำให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตนสามารถลักลอบรันคำสั่งที่เป็นอันตราย (RCE) และยึดควบคุมระบบได้	FortiAuthenticator 6.5, 6.6 และ 8.0
NGINX	• ช่องโหว่ CVE-2026-42945 เกิดจากความผิดพลาดในการจัดการข้อมูลหน่วยความจำระหว่างขั้นตอนการคำนวณ Buffer Size และการเขียนข้อมูลลง Heap Memory ในโมดูล ngx_http_rewrite_module ซึ่งเป็นองค์ประกอบหลักของ NGINX ที่ใช้สำหรับ Rewrite URL การจัดการ Routing และการกำหนดเงื่อนไขของ Web Request ภายใน Web Application ทำให้ผู้ไม่หวังดีสามารถรันโค้ดจากระยะไกล (RCE) เพื่อเข้าควบคุมระบบ หรือทำให้ระบบไม่สามารถให้บริการได้ (Denial of Service: DoS)	NGINX Open Source 1.0.0 - 1.30.0 และ NGINX Plus R32 - R36

ข้อมูลอ้างอิง Fortinet

1. https://nvd.nist.gov/vuln/detail/CVE-2026-26083
2. https://fortiguard.fortinet.com/psirt/FG-IR-26-136
3. https://nvd.nist.gov/vuln/detail/CVE-2026-44277
4. https://fortiguard.fortinet.com/psirt/FG-IR-26-128
5. https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-rce-flaws-in-fortisandbox-and-fortiauthenticator/

ข้อมูลอ้างอิง NginX

1. https://thehackernews.com/2026/05/18-year-old-nginx-rewrite-module-flaw.html
2. https://nvd.nist.gov/vuln/detail/CVE-2026-42945
3. https://depthfirst.com/nginx-rift

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ