วันที่ 21 พฤษภาคม 2569

## Ivanti, Fortinet, SAP, VMware และ n8n ออกแพตช์แก้ช่องโหว่ RCE, SQL Injection และ Privilege Escalation


Ivanti, Fortinet, n8n, SAP และ VMware ได้ออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่หลายรายการ ซึ่งผู้ไม่หวังดีอาจนำไปใช้เพื่อข้ามการยืนยันตัวตน (Authentication Bypass) และรันโค้ดอันตรายบนระบบได้

ช่องโหว่ที่มีความรุนแรงสูงที่สุดในรอบนี้คือช่องโหว่ที่กระทบกับ Ivanti Xtraction หมายเลข CVE-2026-8043 (คะแนน CVSS: 9.6) ซึ่งอาจถูกใช้เพื่อเข้าถึงข้อมูลสำคัญ หรือใช้ในการโจมตีฝั่งผู้ใช้งาน (Client-side Attack)

Ivanti ระบุว่าช่องโหว่ External control of a file name ใน Ivanti Xtraction เวอร์ชันก่อน 2026.2 อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ผ่านการยืนยันตัวตนแล้ว สามารถอ่านไฟล์สำคัญ และเขียนไฟล์ HTML ลงใน Web Directory ได้ ส่งผลให้เกิดการรั่วไหลของข้อมูล และอาจนำไปสู่การโจมตีฝั่งผู้ใช้งาน

ทางด้าน Fortinet ได้เผยแพร่ประกาศด้านความปลอดภัยสำหรับช่องโหว่ระดับ Critical จำนวน 2 รายการ ที่ส่งผลกระทบต่อ FortiAuthenticator, FortiSandbox, FortiSandbox Cloud และ FortiSandbox PaaS ซึ่งอาจนำไปสู่การรันโค้ดอันตรายได้ ดังนี้

- CVE-2026-44277 (คะแนน CVSS: 9.1) – ช่องโหว่ Improper Access Control ใน FortiAuthenticator ซึ่งอาจเปิดโอกาสให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตน สามารถรันโค้ดหรือคำสั่งที่ไม่ได้รับอนุญาตผ่านคำขอที่ถูกสร้างขึ้นมาเป็นพิเศษ (แก้ไขแล้วใน FortiAuthenticator เวอร์ชัน 6.5.7, 6.6.9 และ 8.0.3)
- CVE-2026-26083 (คะแนน CVSS: 9.1) – ช่องโหว่ Missing Authorization ในหน้า WEB UI ของ FortiSandbox, FortiSandbox Cloud และ FortiSandbox PaaS ซึ่งอาจเปิดทางให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตน สามารถรันโค้ดหรือคำสั่งที่ไม่ได้รับอนุญาตผ่าน HTTP Request ได้ (แก้ไขแล้วใน FortiSandbox เวอร์ชัน 4.4.9 และ 5.0.2, FortiSandbox Cloud เวอร์ชัน 5.0.6 และ FortiSandbox PaaS เวอร์ชัน 4.4.9 และ 5.0.2)

ขณะที่ SAP ได้ออกแพตช์แก้ไขช่องโหว่ระดับ Critical จำนวน 2 รายการ ได้แก่

- CVE-2026-34260 (คะแนน CVSS: 9.6) – ช่องโหว่ SQL Injection ใน SAP S/4HANA
- CVE-2026-34263 (คะแนน CVSS: 9.6) – ช่องโหว่ Missing Authentication Check ในระบบตั้งค่าของ SAP Commerce Cloud

Onapsis อธิบายเกี่ยวกับ CVE-2026-34263 ว่าช่องโหว่นี้เกิดจากการตั้งค่าด้านความปลอดภัยที่เปิดกว้างเกินไป รวมถึงลำดับการทำงานของกฎที่ไม่เหมาะสม ทำให้ผู้โจมตีที่ไม่ต้องยืนยันตัวตน สามารถอัปโหลดไฟล์ตั้งค่าที่เป็นอันตรายและฝังโค้ดได้ ส่งผลให้สามารถรันโค้ดบนเซิร์ฟเวอร์ได้ตามต้องการ

ส่วน CVE-2026-34260 อาจถูกใช้เพื่อแทรกคำสั่ง SQL ที่เป็นอันตราย และอาจส่งผลกระทบต่อความลับของข้อมูล (Confidentiality) และความพร้อมใช้งานของระบบ (Availability) อย่างไรก็ตาม ช่องโหว่นี้ไม่ส่งผลต่อความถูกต้องของข้อมูล (Integrity) เนื่องจากโค้ดที่ได้รับผลกระทบอนุญาตให้เข้าถึงข้อมูลแบบอ่านอย่างเดียวเท่านั้น

Pathlock ระบุว่าช่องโหว่นี้เปิดโอกาสให้ผู้โจมตีที่มีสิทธิ์ระดับต่ำและผ่านการยืนยันตัวตนแล้ว สามารถแทรก SQL ผ่านข้อมูลที่ผู้ใช้ควบคุมได้ ซึ่งอาจนำไปสู่การเปิดเผยข้อมูลสำคัญในฐานข้อมูล และทำให้แอปพลิเคชันล่มได้

นอกจากนี้ Broadcom ยังได้ออกแพตช์แก้ไขช่องโหว่ความรุนแรงสูงใน VMware Fusion หมายเลข CVE-2026-41702 (คะแนน CVSS: 7.8) ซึ่งอาจถูกใช้เพื่อยกระดับสิทธิ์เป็นระดับ Root ได้ โดยแก้ไขแล้วในเวอร์ชัน 26H1

Broadcom ระบุว่า VMware Fusion มีช่องโหว่ประเภท TOCTOU (Time-of-check Time-of-use) ที่เกิดขึ้นระหว่างกระบวนการทำงานของไฟล์แบบ SETUID ผู้โจมตีที่มีสิทธิ์ผู้ใช้ภายในเครื่องในระดับไม่ใช่ผู้ดูแลระบบ อาจใช้ช่องโหว่นี้เพื่อยกระดับสิทธิ์เป็น Root บนระบบที่ติดตั้ง Fusion ได้

ปิดท้ายด้วยชุดช่องโหว่ระดับ Critical จำนวน 5 รายการที่กระทบกับ n8n ดังนี้

- CVE-2026-42231 (คะแนน CVSS: 9.4) – ช่องโหว่ในไลบรารี xml2js ที่ใช้ประมวลผล XML Request ใน Webhook Handler ของ n8n ซึ่งอาจทำให้เกิด Prototype Pollution ผ่าน XML Payload ที่ถูกสร้างขึ้นเป็นพิเศษ ส่งผลให้ผู้ใช้ที่มีสิทธิ์สร้างหรือแก้ไข Workflow สามารถรันโค้ดบนเซิร์ฟเวอร์ n8n ได้ (แก้ไขแล้วใน n8n เวอร์ชัน 1.123.32, 2.17.4 และ 2.18.1)
- CVE-2026-42232 (คะแนน CVSS: 9.4) – ผู้ใช้ที่มีสิทธิ์สร้างหรือแก้ไข Workflow อาจใช้ XML Node เพื่อทำ Global Prototype Pollution และนำไปสู่การรันโค้ดบนเซิร์ฟเวอร์ เมื่อใช้งานร่วมกับ Node อื่นที่ได้รับผลกระทบ (แก้ไขแล้วใน n8n เวอร์ชัน 1.123.32, 2.17.4 และ 2.18.1)
- CVE-2026-44791 (คะแนน CVSS: 9.4) – ช่องโหว่ที่สามารถใช้ข้ามการป้องกันของ CVE-2026-42232 และอาจนำไปสู่การรันโค้ดบนเซิร์ฟเวอร์ n8n ได้ (แก้ไขแล้วใน n8n เวอร์ชัน 1.123.43, 2.20.7 และ 2.22.1)

- CVE-2026-44789 (คะแนน CVSS: 9.4) – ผู้ใช้ที่มีสิทธิ์สร้างหรือแก้ไข Workflow สามารถทำ Global Prototype Pollution ผ่านพารามิเตอร์ Pagination ที่ไม่มีการตรวจสอบใน HTTP Request Node ซึ่งอาจนำไปสู่การรันโค้ดบนเซิร์ฟเวอร์ n8n ได้ (แก้ไขแล้วใน n8n เวอร์ชัน 1.123.43, 2.20.7 และ 2.22.1)
- CVE-2026-44790 (คะแนน CVSS: 9.4) – ผู้ใช้ที่มีสิทธิ์สร้างหรือแก้ไข Workflow สามารถฝัง CLI Flags ในกระบวนการ Push ของ Git Node ได้ ทำให้สามารถอ่านไฟล์ใดก็ได้บนเซิร์ฟเวอร์ n8n และอาจนำไปสู่การยึดระบบทั้งหมด (แก้ไขแล้วใน n8n เวอร์ชัน 1.123.43, 2.20.7 และ 2.22.1)

ผู้ผลิตรายอื่นที่ออกแพตช์ด้านความปลอดภัยเพิ่มเติมในช่วงหลายสัปดาห์ที่ผ่านมา เพื่อแก้ไขช่องโหว่ต่างๆ ได้แก่

- ABB
- Adobe
- Amazon Web Services
- AMD
- Apple
- ASUS
- Atlassian
- Axis Communications
- AVEVA
- Canon
- Cisco
- CODESYS
- ConnectWise
- Dell
- Devolutions
- Drupal
- F5
- Fortra
- Foxit Software
- Fujitsu
- GitLab

- GnuTLS
- Google Android และ Pixel
- Google Chrome
- Google Cloud
- Grafana
- Hikvision
- Hitachi Energy
- Honeywell
- HP
- HP Enterprise (รวมถึง Aruba Networking และ Juniper Networks)
- Huawei
- IBM
- Intel
- Jenkins
- Lenovo
- Linux distributions ได้แก่ AlmaLinux, Alpine Linux, Amazon Linux, Arch Linux, Debian, Gentoo, Oracle Linux, Mageia, Red Hat, Rocky Linux, SUSE และ Ubuntu
- MediaTek
- Meta WhatsApp
- Microsoft
- Mitel
- Mitsubishi Electric
- MongoDB
- Moxa
- Mozilla Firefox, Firefox ESR และ Thunderbird
- NVIDIA
- OPPO
- Palo Alto Networks
- Phoenix Contact

- Phoenix Technologies
- Progress Software
- QNAP
- Qualcomm
- React
- Ricoh
- Samsung
- Schneider Electric
- Siemens
- Sophos
- Spring Framework
- Supermicro
- Synology
- Tenable
- TP-Link
- WatchGuard
- Zoom
- และ Zyxel

**ข้อมูลอ้างอิง**

May 18, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/05/ivanti-fortinet-sap-vmware-n8n-patch.html