แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

SAP, Microsoft และ 7-Zip ออก Security Patch เพื่อแก้ไขช่องโหว่หลายรายการ

วันที่แจ้งเตือน 22 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า SAP, Microsoft และ 7-Zip ได้ออก Security Patch เพื่อแก้ไขช่องโหว่ในผลิตภัณฑ์หลายรายการ ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
SAP	1. **ช่องโหว่ CVE-2026-44747** เป็นช่องโหว่ประเภท Memory Corruption ซึ่งทำให้ผู้ไม่หวังดีสามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูล หรือทำให้ระบบไม่สามารถให้บริการได้ 2. **ช่องโหว่ CVE-2026-27690** เป็นช่องโหว่ประเภท HTTP Request Smuggling ที่ส่งผลกระทบต่อการติดตั้ง SAP Approuter ที่ไม่ได้ใช้งานบน Cloud Foundry ทำให้ผู้ไม่หวังดีไม่ต้องผ่านกระบวนการยืนยันตัวตน สามารถส่ง HTTP Request ที่สร้างขึ้น จนทำให้เกิดกระบวนการประมวลผลคำขอและการตอบกลับของระบบไม่สอดคล้องกัน และนำไปสู่การโจมตีรูปแบบอื่นเพิ่มเติมได้ 3. **ช่องโหว่ CVE-2026-44761** เป็นช่องโหว่ประเภท Hardcode Credential เกิดจาก Sample Configuration Script สำหรับการพัฒนาและทดสอบ ซึ่งกำหนดข้อมูลรับรองของ OAuth2 Client เป็นค่าคงที่ ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงหรือแก้ไขข้อมูลได้โดยไม่ได้รับอนุญาต • SAP แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	■ **ช่องโหว่ 1: SAP NetWeaver Application Server ABAP** • KRNL64NUC 7.22 และ 7.22EXT • KRNL64UC 7.22, 7.22EXT และ 7.53 • KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.18, 9.19 และ 9.20 ■ **ช่องโหว่ 2: SAP Approuter Node.js Package เวอร์ชันต่ำกว่า 20.10.0** ■ **ช่องโหว่ 3: SAP Commerce Cloud** • HY_COM 2205 • COM_CLOUD 2211 • COM_CLOUD 2211-JDK21

ข้อมูลอ้างอิง SAP

1. https://nvd.nist.gov/vuln/detail/CVE-2026-44747
2. https://nvd.nist.gov/vuln/detail/CVE-2026-27690
3. https://nvd.nist.gov/vuln/detail/CVE-2026-44761
4. https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html
5. https://www.securityweek.com/sap-patches-critical-vulnerabilities-in-netweaver-approuter-commerce-cloud/

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

SAP, Microsoft และ 7-Zip ออก Security Patch เพื่อแก้ไขช่องโหว่หลายรายการ

วันที่แจ้งเตือน 22 กรกฎาคม 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	• **ช่องโหว่ CVE-2026-50522** เป็นประเภท Deserialization เกิดจากการประมวลผลข้อมูลที่ไม่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถโจมตีหรือสั่งรันโค้ดอันตรายได้จากระยะไกล เพื่อขโมย SharePoint Machine Keys ผ่านคำขอเพียงครั้งเดียวโดยไม่ต้องยืนยันตัวตน และไม่ต้องอาศัยการกระทำของผู้ใช้งาน และยังสามารถเข้าถึงระบบได้ แม้องค์กรจะติดตั้งแพตช์แก้ไขช่องโหว่แล้วก็ตาม • Microsoft แนะนำให้ผู้ใช้ผลิตภัณฑ์อัปเกรดเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ Microsoft SharePoint Server แบบ On-premise
7-Zip	• โปรแกรม 7-Zip ได้ออกเวอร์ชัน 26.02 เพื่อแก้ไขช่องโหว่ประเภท Heap-based Buffer Overflow ซึ่งผู้ไม่หวังดีสามารถสั่งรันโค้ดหรือมัลแวร์บนเครื่องของผู้ใช้งานได้ หากผู้ใช้งานเปิดไฟล์บีบอัดข้อมูล XZ ที่ผู้ไม่หวังดีสร้างขึ้นเพื่อใช้ในการโจมตีแบบ Phishing เพื่อหลอกลวงให้ผู้ใช้เปิดไฟล์ที่แนบมาจากอีเมล หรือการดาวน์โหลดจากเว็บไซต์ จากนั้นจะติดตั้งมัลแวร์ลงในเครื่องของผู้ใช้ และโจมตีเพิ่มเติม • โปรแกรม 7-Zip ไม่มีระบบอัปเดตอัตโนมัติ ผู้ใช้งานจึงต้องดาวน์โหลดและติดตั้งเวอร์ชันล่าสุดด้วยตนเอง	ส่งผลกระทบต่อ 7-Zip เวอร์ชันเก่ากว่า 26.02

ข้อมูลอ้างอิง Microsoft

1. https://nvd.nist.gov/vuln/detail/CVE-2026-50522
2. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522
3. https://securityaffairs.com/195760/security/public-poc-triggers-active-exploitation-of-critical-sharepoint-rce-vulnerability-cve-2026-50522.html

ข้อมูลอ้างอิง 7-Zip

1. https://www.zerodayinitiative.com/advisories/ZDI-26-444/
2. https://www.bleepingcomputer.com/news/security/update-now-7-zip-fixes-rce-flaw-exploitable-with-malicious-archives/