วันที่ 22 กันยายน 2569

## Cisco แจ้งเตือนช่องโหว่ Zero-Day ใหม่ใน ISE ที่สามารถหลบเลี่ยงการยืนยันตัวตน (CVSS 10.0) และกำลังถูกโจมตี


Cisco ได้ออกมาแจ้งเตือนถึงช่องโหว่ด้านความปลอดภัยระดับรุนแรงสูงสุดช่องโหวใหม่ที่ส่งผลกระทบต่อ Identity Services Engine (ISE) และขณะนี้กำลังถูกนำไปใช้ในการโจมตีจริง โดยช่องโหว่นี้มีหมายเลข CVE-2026-76460 และมีคะแนนความรุนแรง CVSS 10.0 โดยอาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ไม่จำเป็นต้องผ่านการยืนยันตัวตน สามารถหลบเลี่ยงกระบวนการยืนยันตัวตนได้

Cisco ระบุว่าช่องโหว่นี้เกิดจากการควบคุมการยืนยันตัวตนที่ไม่เพียงพอบน API endpoint ผู้โจมตีสามารถใช้ช่องโหว่นี้โดยส่งคำขอที่ถูกสร้างขึ้นเป็นพิเศษไปยัง API endpoint ที่ได้รับผลกระทบ หากโจมตีสำเร็จ ผู้โจมตีอาจเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาตผ่านการหลบเลี่ยงหน้าจัดการระบบบนเว็บ ช่องโหว่นี้ส่งผลกระทบต่อ Cisco ISE และ Cisco ISE Passive Identity Connector (ISE-PIC) โดยไม่ขึ้นอยู่กับการตั้งค่าของอุปกรณ์ และได้รับการแก้ไขแล้วในเวอร์ชันต่อไปนี้

- 3.1 - แก้ไขแล้วใน 3.1 Patch 12
- 3.2 - แก้ไขแล้วใน 3.2 Patch 11
- 3.3 - แก้ไขแล้วใน 3.3 Patch 12
- 3.4 - แก้ไขแล้วใน 3.4 Patch 7
- 3.51 - แก้ไขแล้วใน 3.5 Patch 4

Cisco ระบุว่า พบการโจมตีช่องโหว่นี้เกิดขึ้นจริงแล้วและแนะนำให้ลูกค้าอัปเกรดซอฟต์แวร์ไปเป็นเวอร์ชันที่ได้รับ การแก้ไขเพื่อรับมือกับความเสี่ยงดังกล่าว อย่างไรก็ตาม บริษัทไม่ได้เปิดเผยรายละเอียดเกี่ยวกับลักษณะของการโจมตี หรือระบุว่ากลุ่มใดอยู่เบื้องหลังการโจมตี

สำหรับตัวบ่งชี้การบุกรุก (IoCs) Cisco แนะนำให้ผู้ใช้งานตรวจสอบไฟล์ access.log และค้นหาชื่อผู้ใช้ที่น่าสงสัย หากอุปกรณ์เป็นส่วนหนึ่งของระบบที่มีการกระจายการทำงาน จำเป็นต้องตรวจสอบ Log ของทุก Node โดย Cisco ได้แนะนำคำสั่งต่อไปนี้สำหรับตรวจหาชื่อผู้ใช้ที่ไม่ควรปรากฏในระบบ

```
admin#show logging application ise-kong/access.log | include dummyuser
```

หากพบรายการใดๆ จากคำสั่งดังกล่าว อาจเป็นสัญญาณว่าระบบถูกโจมตีหรือมีการใช้งานช่องโหว่ หากพบกิจกรรมในลักษณะนี้ Cisco แนะนำให้ติดตั้งระบบของ Node ที่ได้รับผลกระทบใหม่ทั้งหมด และกู้คืนการตั้งค่าจากข้อมูลสำรองตามความจำเป็น

Cisco ระบุเพิ่มเติมว่า หลังจากโจมตีช่องโหว่นี้สำเร็จ ผู้โจมตีอาจสามารถสั่งให้ระบบทำงานด้วยสิทธิ์ระดับ Root ได้ เนื่องจากผู้โจมตีมีสิทธิ์ในระดับสูงดังกล่าว หลักฐานการโจมตีและตัวบ่งชี้การบุกรุกต่างๆ อาจถูกลบหรือซ่อนเพื่อไม่ให้ตรวจพบได้ Cisco ยังย้ำว่าไม่มีวิธีแก้ไขชั่วคราวสำหรับช่องโหว่นี้ แต่ในด้านการลดความเสี่ยง ลูกค้าสามารถใช้ Infrastructure Access Control Lists (iACLs) เพื่อกำหนดให้มีเพียงการรับส่งข้อมูลด้านการจัดการระบบและการควบคุมที่จำเป็นเท่านั้น ที่สามารถเข้าถึงอุปกรณ์ที่ได้รับผลกระทบได้

เมื่อวันที่ 16 กันยายน 2026 หน่วยงาน Cybersecurity and Infrastructure Security Agency (CISA) ของสหรัฐฯ ได้เพิ่ม CVE-2026-76460 เข้าไปในรายการ Known Exploited Vulnerabilities (KEV) ซึ่งกำหนดให้หน่วยงาน Federal Civilian Executive Branch (FCEB) ดำเนินการติดตั้งแพตช์ภายในวันที่ 19 กันยายน 2026

การเปิดเผยช่องโหว่นี้เกิดขึ้นเพียงไม่กี่วันหลังจาก Cisco แจ้งเตือนว่าช่องโหว่ระดับรุนแรงที่ส่งผลกระทบต่อ AsyncOS Software สำหรับ Cisco Secure Email Gateway (CVE-2026-76461, CVSS score: 9.8) กำลังถูกนำไปใช้โจมตีจริงบนอินเทอร์เน็ต

นอกเหนือจาก CVE-2026-76460 แล้ว Cisco ยังได้ออกแพตช์แก้ไขช่องโหว่ด้านความปลอดภัยระดับรุนแรงอีกหลายรายการในผลิตภัณฑ์ต่างๆ ของบริษัท โดยบางรายการเป็นการปรับปรุงด้านความปลอดภัยที่ออกมาเป็นส่วนหนึ่งของการตรวจสอบระบบอย่างต่อเนื่อง จาก CVE ใหม่ทั้งหมด 77 รายการที่ถูกเปิดเผยเมื่อวันพุธ มี 41 รายการที่ส่งผลกระทบต่อ ISE และอีก 28 รายการส่งผลกระทบต่อผลิตภัณฑ์ Secure Firewall โดยมีรายละเอียดโดยสรุปดังนี้

- **CVE-2026-20176 (CVSS score: 9.9), CVE-2026-20211 (CVSS score: 9.1), CVE-2026-20307 (CVSS score: 9.1)** - ช่องโหว่หลายรายการใน ISE ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ผ่านการยืนยันตัวตนแล้ว สามารถสั่งให้ระบบปฏิบัติการของอุปกรณ์ที่ได้รับผลกระทบทำงานตามคำสั่งที่ผู้โจมตีต้องการได้ โดยผู้โจมตีจำเป็นต้องมีบัญชีผู้ดูแลระบบที่ถูกต้อง
- **CVE-2026-76423 (CVSS score: 10.0), CVE-2026-76424, CVE-2026-76425, CVE-2026-76426, CVE-2026-76427, CVE-2026-76428** - ช่องโหว่หลายรายการใน ISE และ Cisco ISE Passive Identity Connector (ISE-PIC) ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลสามารถหลบเลี่ยงการยืนยันตัวตนของ REST API, สั่งให้ระบบทำงานตามคำสั่งที่ต้องการจากระยะไกล, แทรกคำสั่ง SQL หรือโจมตีผ่าน XML External Entity (XXE) บนอุปกรณ์ที่ได้รับผลกระทบ
- **CVE-2026-20282 (CVSS score: 9.1), CVE-2026-20283, CVE-2026-20284** - ช่องโหว่หลายรายการใน ISE ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ผ่านการยืนยันตัวตนแล้ว สามารถแทรกคำสั่ง SQL, แก้ไขข้อมูล หรือสั่งให้ระบบปฏิบัติการของอุปกรณ์ทำงานตามคำสั่งที่ผู้โจมตีต้องการ

- **CVE-2026-20305 (CVSS score: 9.1), CVE-2026-20306 (CVSS score: 9.1)** - ช่องโหว่หลายรายการใน ISE และ ISE-PIC ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ผ่านการยืนยันตัวตนแล้ว สามารถแทรกคำสั่งเข้าไปในระบบและสั่งให้ระบบทำงานตามคำสั่งต่างๆ ด้วยสิทธิ์ระดับ Root โดยผู้โจมตีจำเป็นต้องมีบัญชีผู้ดูแลระบบที่ถูกต้อง
- **CVE-2026-20322 (CVSS score: 9.9), CVE-2026-20325 (CVSS score: 9.9), CVE-2026-20326 (CVSS score: 9.8), CVE-2026-20360, CVE-2026-20361, CVE-2026-76409** - ช่องโหว่หลายรายการใน Cisco Nexus Dashboard ที่อาจทำให้ผู้โจมตีสามารถแทรกคำสั่ง, หลบเลี่ยงการยืนยันตัวตนหรือการตรวจสอบสิทธิ์ และเข้าถึงข้อมูลที่ไม่ควรเข้าถึงได้
- **CVE-2026-20130 (CVSS score: 10.0), CVE-2026-20192 (CVSS score: 10.0), CVE-2026-20194 (CVSS score: 9.1), CVE-2026-20234 (CVSS score: 9.9), CVE-2026-20237 (CVSS score: 9.9), CVE-2026-20287** - ช่องโหว่หลายรายการใน ISE และ ISE-PIC ที่อาจทำให้ผู้โจมตีสามารถแทรกคำสั่ง, หลบเลี่ยงการยืนยันตัวตนหรือการตรวจสอบสิทธิ์ และเข้าถึงข้อมูลที่ไม่ควรเข้าถึงได้
- **CVE-2026-20329 (CVSS score: 9.9), CVE-2026-20330 (CVSS score: 9.9), CVE-2026-20331 (CVSS score: 9.6), CVE-2026-20332 (CVSS score: 9.0), CVE-2026-20333, CVE-2026-20334, CVE-2026-20335, CVE-2026-20336** - ช่องโหว่หลายรายการใน Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software และ Cisco Secure Firewall Management Center (FMC) Software ซึ่งถูกจัดกลุ่มตามประเภทของช่องโหว่ (CWE) ครอบคลุมปัญหาต่างๆ เช่น การจัดการสถานการณ์ผิดปกติที่ไม่เหมาะสม, การควบคุมการเข้าถึงที่ไม่เหมาะสม, การทำงานที่ไม่สอดคล้องกับมาตรฐานการเขียนโปรแกรม และการควบคุมทรัพยากรของระบบตลอดอายุการใช้งานที่ไม่เหมาะสม
- **CVE-2026-76412, CVE-2026-76413, CVE-2026-76420 (CVSS score: 9.0)** - ช่องโหว่หลายรายการใน Cisco Secure Firewall Management Center (FMC) Software ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลสามารถเข้าถึงระบบด้วยสิทธิ์ระดับ Root และปลอมแปลงหรือสวมรอย Session ของผู้ใช้งาน
- **CVE-2026-20324 (CVSS score: 9.9)** - ช่องโหว่ในโปรโตคอล sftunnel ซึ่งใช้สำหรับการสื่อสารระหว่างอุปกรณ์ของ FMC Software ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ผ่านการยืนยันตัวตนแล้ว สามารถสั่งให้ระบบทำงานตามคำสั่งที่ต้องการด้วยสิทธิ์ระดับ Root
- **CVE-2026-20340, CVE-2026-20341 (CVSS score: 9.1), CVE-2026-20342, CVE-2026-20343, CVE-2026-20344** - ช่องโหว่หลายรายการใน FMC Software ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลสามารถเข้าถึงระบบด้วยสิทธิ์ระดับ Root, ดาวน์โหลดไฟล์สำคัญ, แทรกคำสั่ง SQL หรือทำให้ระบบหยุดให้บริการ (DoS)
- **CVE-2026-20242 (CVSS score: 9.8)** - ช่องโหว่ในฟีเจอร์ External Database Access ของ FMC Software ที่อาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ไม่จำเป็นต้องผ่านการยืนยันตัวตน สามารถสั่งให้ระบบทำงานตามคำสั่งที่ต้องการด้วยสิทธิ์ระดับ Root

- **CVE-2026-20353 (CVSS score: 9.8), CVE-2026-76440 (CVSS score: 9.8), CVE-2026-76441 (CVSS score: 9.8), CVE-2026-76442 (CVSS score: 9.8), CVE-2026-76443** - ช่องโหว่หลายรายการใน Cisco Secure Email Gateway และ Cisco Secure Email and Web Manager ที่อาจนำไปสู่การเข้าถึงไฟล์นอกเหนือจากที่ได้รับอนุญาต, การหลบเลี่ยงการยืนยันตัวตนหรือการตรวจสอบสิทธิ์, การใช้ทรัพยากรของระบบจนหมด และการแทรกคำสั่งเข้าสู่ระบบ

แม้ว่าช่องโหว่เหล่านี้จะยังไม่มีรายการใดถูกระบุว่ากำลังถูกนำไปใช้โจมตีจริง แต่ผู้ใช้งานควรติดตั้งแพตช์แก้ไขโดยเร็ว เนื่องจากช่องโหว่เหล่านี้มีความรุนแรงสูง และหลายรายการอาจเปิดช่องให้ผู้โจมตีสามารถสั่งให้ระบบทำงานตามคำสั่งที่ต้องการได้

**ข้อมูลอ้างอิง**

Sep 17, 2026 By Ravie Lakshmanan

- https://thehackernews.com/2026/09/cisco-warns-of-new-zero-day-ise-auth.html