วันที่ 18 มกราคม 2569

Cisco ออกแพตช์อุดช่องโหว่ Zero-Day RCE ที่ถูกกลุ่ม APT ที่เชื่อมโยงกับจีนใช้โจมตี Secure Email Gateway

เมื่อวันพฤหัสบดีที่ผ่านมา Cisco ได้ประกาศออกอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ความรุนแรงระดับสูงสุดที่ส่งผลกระทบต่อ Cisco AsyncOS Software สำหรับ Cisco Secure Email Gateway และ Cisco Secure Email and Web Manager หลังจากที่ก่อนหน้านี้บริษัทได้เปิดเผยว่าช่องโหว่ดังกล่าวได้ถูกกลุ่มภัยคุกคามขั้นสูง (APT) ที่เชื่อมโยงกับจีนภายใต้รหัส UAT-9686 นำไปใช้โจมตีจริงในลักษณะ Zero-day เป็นที่เรียบร้อยแล้ว

เจาะลึกรายละเอียดช่องโหว่ CVE-2025-20393

ช่องโหว่นี้ถูกติดตามด้วยรหัส CVE-2025-20393 และได้รับคะแนนความรุนแรงเต็ม CVSS: 10.0 โดยเป็นช่องโหว่ประเภทการรันคำสั่งจากระยะไกล (Remote Command Execution - RCE) ที่เกิดจากการตรวจสอบคำขอ HTTP ที่ไม่รัดกุมพอในฟีเจอร์ Spam Quarantine ซึ่งหากผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นี้ได้สำเร็จ จะสามารถสั่งรันคำสั่งใดๆ ก็ได้ด้วยสิทธิ์ระดับ root บนระบบปฏิบัติการของอุปกรณ์ที่ได้รับผลกระทบ

เงื่อนไขสำคัญในการโจมตี: อย่างไรก็ตาม การโจมตีจะประสบความสำเร็จได้ก็ต่อเมื่ออุปกรณ์มีเงื่อนไขครบถ้วนทั้ง 3 ข้อ ดังนี้:

1. อุปกรณ์ต้องใช้งาน Cisco AsyncOS Software ในเวอร์ชันที่มีช่องโหว่
2. มีการเปิดใช้งานฟีเจอร์ Spam Quarantine
3. ฟีเจอร์ Spam Quarantine ถูกตั้งค่าให้สามารถเข้าถึงได้จากอินเทอร์เน็ต

เบื้องหลังแคมเปญโจมตีโดยกลุ่ม UAT-9686

เมื่อเดือนที่ผ่านมา Cisco เปิดเผยหลักฐานสำคัญว่ากลุ่ม UAT-9686 ได้เริ่มใช้ช่องโหว่นี้โจมตีเป้าหมายมาตั้งแต่ช่วงปลายเดือนพฤศจิกายน 2025 โดยมีการติดตั้งชุดเครื่องมือที่ซับซ้อน ได้แก่:

- เครื่องมือสำหรับทำ Tunneling: เช่น ReverseSSH (หรือที่รู้จักในชื่อ AquaTunnel) และ Chisel
- เครื่องมือทำความสะอาดร่องรอย: ชื่อว่า AquaPurge ซึ่งใช้สำหรับลบหรือทำความสะอาดบันทึกเหตุการณ์ (log) เพื่ออำพรางการโจมตี
- การฝังตัว (Persistence): มีการติดตั้งแบ็กดอร์ขนาดเล็กที่เขียนด้วยภาษา Python ชื่อว่า AquaShell ซึ่งมีความสามารถในการรับคำสั่งที่ถูกเข้ารหัส และนำไปประมวลผลหรือรันบนระบบได้ทันที

รายละเอียดเวอร์ชันที่ได้รับการแก้ไข (Patch Versions)

ปัจจุบัน Cisco ได้แก้ไขช่องโหว่นี้เรียบร้อยแล้ว พร้อมทั้งลบกลไกการฝังตัวถาวร (persistence) ที่ตรวจพบจากแคมเปญการโจมตีดังกล่าวออกจากอุปกรณ์ด้วย โดยมีรายละเอียดเวอร์ชันที่ต้องอัปเดตดังนี้:

1. Cisco Email Security Gateway:

- Release 14.2 และก่อนหน้า: แก้ไขแล้วในเวอร์ชัน 15.0.5-016
- Release 15.0: แก้ไขแล้วในเวอร์ชัน 15.0.5-016
- Release 15.5: แก้ไขแล้วในเวอร์ชัน 15.5.4-012
- Release 16.0: แก้ไขแล้วในเวอร์ชัน 16.0.4-016

2. Secure Email and Web Manager:

- Release 15.0 และก่อนหน้า: แก้ไขแล้วในเวอร์ชัน 15.0.2-007
- Release 15.5: แก้ไขแล้วในเวอร์ชัน 15.5.4-007
- Release 16.0: แก้ไขแล้วในเวอร์ชัน 16.0.4-010

แนวทางการเสริมความปลอดภัย (Hardening) เพิ่มเติม

นอกจากฟการติดตั้งแพตช์แล้ว Cisco ยังแนะนำให้ลูกค้าปฏิบัติตามแนวทางการ Hardening เพื่อป้องกันความเสี่ยงเพิ่มเติม ดังนี้:

- ป้องกันไม่ให้อุปกรณ์เข้าถึงได้จากเครือข่ายที่ไม่ปลอดภัย
- วางอุปกรณ์ไว้ภายหลังไฟร์วอลล์ (Firewall)
- ตรวจสอบทราฟฟิกจาก Web Log อย่างสม่ำเสมอเพื่อหาพฤติกรรมที่ผิดปกติ
- ปิดการใช้งาน HTTP สำหรับพอร์ทัลผู้ดูแลระบบหลัก (Main Administration Portal)
- ปิดบริการเครือข่ายที่ไม่จำเป็น

- บังคับใช้การยืนยันตัวตนที่มีความแข็งแรงสำหรับผู้ใช้งาน (เช่น SAML หรือ LDAP)
- เปลี่ยนรหัสผ่านผู้ดูแลระบบเริ่มต้นให้มีความปลอดภัยและซับซ้อนมากยิ่งขึ้น

ข้อมูลอ้างอิง

Jan 16, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/01/cisco-patches-zero-day-rce-exploited-by.html