วันที่ 6 มีนาคม 2569

Cisco แจ้งเตือน! พบการโจมตีจริงผ่านช่องโหว่ใหม่บน Catalyst SD-WAN Manager

บริษัทยักษ์ใหญ่ด้านเครือข่ายอย่าง Cisco ออกมาเปิดเผยการตรวจพบช่องโหว่เพิ่มเติมอีก 2 รายการ ที่ส่งผลกระทบต่อ Cisco Catalyst SD-WAN Manager (หรือชื่อเดิมคือ SD-WAN vManage) โดยสิ่งที่น่ากังวลที่สุดคือช่องโหว่เหล่านี้กำลังถูกกลุ่มผู้ไม่หวังดีนำไปใช้โจมตีจริงในปัจจุบัน

เจาะลึกรายละเอียดช่องโหว่

ช่องโหว่แรกคือ **CVE-2026-20122 (คะแนน CVSS: 7.1)** ซึ่งเป็นช่องโหว่ประเภทเขียนทับไฟล์โดยไม่ได้รับอนุญาต (Arbitrary File Overwrite) จุดนี้เปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ผ่านการยืนยันตัวตนแล้ว สามารถเขียนทับไฟล์ใดๆ บนระบบไฟล์ของเครื่องได้ อย่างไรก็ตาม การโจมตีจะสำเร็จได้นั้น ผู้โจมตีต้องมีบัญชีผู้ใช้ที่มีสิทธิ์อย่างน้อยระดับ อ่านอย่างเดียว (Read-only) และต้องสามารถเข้าถึง API ของระบบที่ได้รับผลกระทบได้

อีกหนึ่งรายการคือ **CVE-2026-20128 (คะแนน CVSS: 5.5)** ซึ่งเป็นช่องโหว่ด้านการเปิดเผยข้อมูล (Information Disclosure) ที่อาจทำให้ผู้โจมตีที่ผ่านการยืนยันตัวตนและอยู่ในระบบอยู่แล้ว สามารถยกระดับสิทธิ์ของตนเองขึ้นเป็นผู้ใช้ของ Data Collection Agent (DCA) บนระบบได้ โดยผู้โจมตีจำเป็นต้องมีบัญชี vManage ที่ถูกต้องบนระบบดังกล่าวเพื่อใช้เป็นช่องทางในการโจมตี

การปล่อยแพตช์และเวอร์ชันที่ได้รับการแก้ไข

Cisco ได้เร่งปล่อยแพตช์สำหรับอุดช่องโหว่เหล่านี้ รวมถึงรายการอื่นๆ อย่าง CVE-2026-20126, CVE-2026-20129 และ CVE-2026-20133 ไปเมื่อปลายเดือนที่ผ่านมา โดยซอฟต์แวร์เวอร์ชันที่ผู้ใช้งานควรเปลี่ยนไปใช้มีดังนี้:

- **เวอร์ชันต่ำกว่า 20.9.1:** แนะนำให้ย้ายไปใช้เวอร์ชันที่ได้รับการแก้ไขทันที
- **เวอร์ชัน 20.9:** แก้ไขแล้วในเวอร์ชัน 20.9.8.2

- **เวอร์ชัน 20.11:** แก้ไขแล้วในเวอร์ชัน **20.12.6.1**
- **เวอร์ชัน 20.12:** แก้ไขแล้วในเวอร์ชัน **20.12.5.3 และ 20.12.6.1**
- **เวอร์ชัน 20.13, 20.14 และ 20.15:** แก้ไขแล้วในเวอร์ชัน **20.15.4.2**
- **เวอร์ชัน 20.16 และ 20.18:** แก้ไขแล้วในเวอร์ชัน **20.18.2.1**

สถานการณ์การโจมตีและข้อควรปฏิบัติ

ทีม Cisco PSIRT ระบุว่า "ในเดือนมีนาคม 2026 ทีมงานได้รับทราบถึงการนำช่องโหว่ CVE-2026-20128 และ CVE-2026-20122 ไปใช้โจมตีจริงแล้ว" ทว่าทางบริษัทยังไม่ได้ให้รายละเอียดเชิงลึกเกี่ยวกับขอบเขตความเสียหายหรือกลุ่มผู้อยู่เบื้องหลังเหตุการณ์นี้

เนื่องจากมีการโจมตีเกิดขึ้นจริง ผู้ใช้งานจึงควรอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุดโดยเร็วที่สุด และควรดำเนินมาตรการความปลอดภัยเพิ่มเติมเพื่อป้องกันความเสี่ยง ดังนี้:

- จำกัดการเข้าถึง: ควบคุมการเข้าถึงจากเครือข่ายที่ไม่ปลอดภัยและวางอุปกรณ์ไว้หลังไฟร์วอลล์
- ปิดช่องทางที่ไม่จำเป็น: ปิดการใช้งาน HTTP สำหรับพอร์ทัลผู้ดูแลระบบ และปิดบริการเครือข่ายอื่นๆ เช่น HTTP และ FTP หากไม่มีความจำเป็นต้องใช้งาน
- ยกระดับความปลอดภัยพื้นฐาน: เปลี่ยนรหัสผ่านผู้ดูแลระบบเริ่มต้นทันที
- เฝ้าระวังอย่างต่อเนื่อง: หมั่นตรวจสอบทราฟฟิกใน Log เพื่อหาการเชื่อมต่อที่ผิดปกติทั้งขาเข้าและขาออกจากระบบ

เกาะติดความเคลื่อนไหวภัยคุกคามต่อเนื่อง

การเปิดเผยข้อมูลครั้งนี้เกิดขึ้นต่อเนื่องจากสัปดาห์ก่อน ซึ่ง Cisco เพิ่งพบช่องโหว่ระดับวิกฤต CVE-2026-20127 (คะแนน CVSS: 10.0) ใน Catalyst SD-WAN Controller และ Manager ที่ถูกกลุ่มภัยคุกคามไซเบอร์นามว่า UAT-8616 ใช้โจมตีเพื่อสร้างช่องทางเข้าถึงระบบอย่างต่อเนื่องภายในองค์กร

นอกจากนี้ ในสัปดาห์เดียวกัน Cisco ยังได้แก้ไขช่องโหว่ระดับรุนแรงสูงสุดอีกสองรายการใน Cisco Secure Firewall Management Center ได้แก่ CVE-2026-20079 และ CVE-2026-20131 (คะแนน CVSS: 10.0) ซึ่งอาจเปิดโอกาสให้ผู้โจมตีจากระยะไกลที่ไม่ต้องยืนยันตัวตน สามารถข้ามขั้นตอนการตรวจสอบและรันโค้ด Java ใดๆ ด้วยสิทธิ์ Root บนอุปกรณ์ได้โดยตรง

ข้อมูลอ้างอิง

Mar 5, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/03/cisco-confirms-active-exploitation-of.html