วันที่ 25 พฤษภาคม 2569

Cisco ออกอัปเดตแก้ไขช่องโหว่ความรุนแรงสูงสุดระดับ CVSS 10.0 ที่ส่งผลกระทบต่อ Secure Workload

Cisco ออกอัปเดตแก้ไขช่องโหว่ความรุนแรงสูงสุดระดับ CVSS 10.0 ที่ส่งผลกระทบต่อ Secure Workload ซึ่งอาจเปิดทางให้ผู้ไม่หวังดีจากภายนอกที่ไม่ได้ยืนยันตัวตน สามารถเข้าถึงข้อมูลสำคัญได้

รายละเอียดช่องโหว่และการทำงาน

ช่องโหว่นี้ถูกติดตามในรหัส CVE-2026-20223 (คะแนน CVSS: 10.0) โดยเกิดจากการตรวจสอบและยืนยันตัวตนที่ ไม่เพียงพอในการเข้าถึง REST API endpoints

Cisco ระบุว่าผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นี้ได้ หากสามารถส่ง API request ที่ถูกสร้างขึ้นมาเป็นพิเศษไปยัง endpoint ที่ได้รับผลกระทบ และหากโจมตีสำเร็จ ผู้โจมตีอาจสามารถอ่านข้อมูลสำคัญ รวมถึงแก้ไขการตั้งค่าข้าม tenant ได้ โดยใช้สิทธิ์ระดับ Site Admin

ผลกระทบและแนวทางการแก้ไข

ปัญหาดังกล่าวส่งผลกระทบต่อ Cisco Secure Workload Cluster Software ทั้งในรูปแบบ SaaS และการติดตั้งใช้งานภายในองค์กร (on-premises) โดยไม่ขึ้นอยู่กับการตั้งค่าอุปกรณ์ และ Cisco ระบุว่า ขณะนี้ยังไม่มีวิธีป้องกันชั่วคราว (workaround) ที่สามารถลดผลกระทบของช่องโหว่นี้ได้ ช่องโหว่นี้ได้รับการแก้ไขแล้วในเวอร์ชันดังต่อไปนี้

- Cisco Secure Workload Release 3.9 และก่อนหน้า: แนะนำให้อัปเกรดไปยังเวอร์ชันที่ได้รับการแก้ไข
- Cisco Secure Workload Release 3.10: แก้ไขแล้วในเวอร์ชัน 3.10.8.3
- Cisco Secure Workload Release 4.0: แก้ไขแล้วในเวอร์ชัน 4.0.3.17

ที่มาและการตรวจพบช่องโหว่

บริษัทผู้ผลิตอุปกรณ์เครือข่ายรายนี้ระบุว่า พบช่องโหว่ดังกล่าวระหว่างการทดสอบความปลอดภัยภายในองค์กร และปัจจุบันยังไม่พบหลักฐานว่าถูกนำไปใช้โจมตีจริงในระบบภายนอก

การเปิดเผยข้อมูลครั้งนี้เกิดขึ้นเพียงหนึ่งสัปดาห์หลังจากที่ Cisco เปิดเผยว่า ช่องโหว่ร้ายแรงระดับสูงสุดอีกตัวหนึ่งใน Catalyst SD-WAN Controller ซึ่งเป็นช่องโหว่ bypass การยืนยันตัวตน (CVE-2026-20182, คะแนน CVSS: 10.0) ถูกใช้โจมตีโดยกลุ่มภัยคุกคามชื่อ UAT-8616 เพื่อเข้าถึงระบบ SD-WAN โดยไม่ได้รับอนุญาต

ข้อมูลอ้างอิง

วันที่ May 22, 2026, By Ravie Lakshmanan

https://thehackernews.com/2026/05/cisco-patches-cvss-100-secure-workload.html