

วันที่ 1 ตุลาคม 2569

Cisco เตือนผู้โจมตีกำลังใช้ช่องโหว่ร้ายแรงเพื่อขโมยการยืนยันตัวตนใน SD-WAN Manager



Cisco เปิดตัวเมื่อวันที่ 30 กันยายนว่า ผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ Zero-Day ระดับร้ายแรงตัวใหม่ใน Cisco Catalyst SD-WAN Manager ซึ่งเป็นระบบที่องค์กรใช้สำหรับจัดการเครือข่าย Cisco SD-WAN ช่องโหว่นี้มีหมายเลข CVE-2026-76504 และอาจเปิดทางให้ผู้โจมตีจากระยะไกลที่ไม่มีสิทธิ์เข้าสู่ระบบ สามารถใช้ API ของ Manager ในสิทธิ์ของผู้ดูแลระบบได้ Cisco ได้ออกเวอร์ชันที่แก้ไขช่องโหว่นี้แล้ว และยังไม่มียูสแก้ไขชั่วคราว โดยช่องโหว่นี้มีคะแนนความรุนแรง CVSS 9.8 จาก 10.0 และอยู่ในส่วนของ API ที่เกี่ยวข้องกับการจัดการเซชันการเข้าสู่ระบบ

สาเหตุของช่องโหว่มาจาก Manager จัดการการเข้ารหัส URI ในคำขอ HTTP ที่ไม่ถูกต้อง ทำให้ผู้โจมตีสามารถสร้างคำขอที่ออกแบบมาเป็นพิเศษเพื่อหลบเลี่ยงการยืนยันตัวตน ซึ่งเดิมกำหนดให้เข้าถึงได้เฉพาะ API Endpoint หนึ่งเท่านั้น ผู้โจมตีไม่จำเป็นต้องมีบัญชีหรือข้อมูลสำหรับเข้าสู่ระบบ เพียงสามารถส่งคำขอดังกล่าวไปยัง API ของ Manager ได้ก็สามารถโจมตีได้ โดย Cisco ได้ระบุว่า Manager ที่เปิดให้เข้าถึงจากอินเทอร์เน็ตมีความเสี่ยงที่จะถูกยึดระบบ เนื่องจากโดยค่าเริ่มต้นบัญชีผู้ดูแลระบบจะมีบทบาท netadmin ซึ่งสามารถดำเนินการต่างๆ บนอุปกรณ์ได้ทั้งหมด

Cisco ระบุว่า Product Security Incident Response Team (PSIRT) "รับทราบว่ามีช่องโหว่ที่กำลังถูกนำไปใช้โจมตีจริง" ในเดือนกันยายน 2026 โดยพบช่องโหว่นี้ระหว่างที่ทีม Technical Assistance Center (TAC) ของ Cisco กำลังให้ความช่วยเหลือลูกค้าจากกรณีแจ้งปัญหา อย่างไรก็ตาม ในประกาศ Cisco ไม่ได้ระบุว่ามียูสการค้าที่ร้ายแรงที่ถูกโจมตี การโจมตีเริ่มขึ้นเมื่อใด ใครเป็นผู้โจมตี หรือผู้โจมตีใช้สิทธิ์ที่ได้มาเพื่อทำอะไรกับระบบ

ช่องโหว่ที่ส่งผลกระทบต่อ SD-WAN Manager โดยไม่ขึ้นอยู่กับรูปแบบการตั้งค่าของระบบ และไม่มีผลิตภัณฑ์อื่นที่ถูกระบุว่าได้รับผลกระทบ โดยเวอร์ชันแรกที่ได้รับการแก้ไขในแต่ละ Release Train มีดังนี้

Release train	First fixed release
Earlier than 20.9	Migrate to a fixed release
20.9	20.9.10.1
20.12	20.12.8.2
20.15	20.15.6.1
20.18	20.18.4.1
26.1	26.1.2.1
26.2	26.2.1

CVE-2026-76504 เป็นคนละช่องโหว่กับช่องโหว่ของ Cisco SD-WAN อีก 3 รายการที่ได้รับการแก้ไขไปก่อนหน้านี้ ได้แก่ CVE-2026-20182 ในเดือนพฤษภาคม และ CVE-2026-20245 กับ CVE-2026-20262 ในเดือนมิถุนายน

เมื่อเปรียบเทียบประกาศด้านความปลอดภัยของช่องโหว่เหล่านี้ พบว่าเวอร์ชันที่แก้ไขปัญหาดังกล่าวทั้งหมดเก่ากว่าเวอร์ชันที่ระบุไว้ในตารางข้างต้น ดังนั้น หาก Manager ถูกอัปเดตครั้งล่าสุดเพื่อแก้ไขช่องโหว่ในเดือนพฤษภาคมหรือมิถุนายน ก็ยังจำเป็นต้องอัปเดตเพื่อแก้ไขช่องโหว่นี้เพิ่มเติม

ในประกาศครั้งนี้ไม่ได้รับ Release Train 20.10, 20.11, 20.13, 20.14 หรือ 20.16 ซึ่งเป็นเวอร์ชันที่ Cisco เคยระบุไว้ในประกาศเดือนพฤษภาคม นอกจากนี้ ประกาศดังกล่าวยังไม่ได้รับถึง Cisco SD-WAN Cloud-Pro และ Cisco SD-WAN for Government (FedRAMP) ซึ่งเป็นรูปแบบการใช้งานที่ถูกกล่าวถึงในประกาศเดือนพฤษภาคมและมิถุนายน

สำหรับ Cisco SD-WAN Cloud (Cisco Managed) ได้รับการแก้ไขแล้วในเวอร์ชัน 20.15.605 ดังนั้นลูกค้าที่ใช้งานเวอร์ชันนี้ไม่จำเป็นต้องดำเนินการใดเพิ่มเติม

สำหรับ Manager ที่ติดตั้งภายในองค์กร (On-Premises) และยังไม่ได้อัปเกรด Cisco แนะนำให้จำกัดการเข้าถึงจากเครือข่ายที่ไม่ปลอดภัย เช่น อินเทอร์เน็ต จนกว่าจะดำเนินการอัปเดต หากจำเป็นต้องเปิดให้เข้าถึงผ่านอินเทอร์เน็ต ควรอนุญาตเฉพาะเครื่องหรือระบบที่รู้จักและเชื่อถือได้เท่านั้น และควรวางส่วนประกอบที่ใช้ควบคุมระบบไว้หลัง Firewall

สำหรับ Cisco Catalyst SD-WAN Cloud Hosted มีการใช้มาตรการป้องกันดังกล่าวไว้อยู่แล้ว โดย Cisco ระบุว่ามาตรการนี้สามารถป้องกันการโจมตีได้จากการทดสอบในสภาพแวดล้อมจำลอง อย่างไรก็ตาม Cisco แนะนำให้ลูกค้าประเมินผลกระทบต่อเครือข่ายของตนเองก่อนนำมามาตรการดังกล่าวไปใช้งาน

คู่มือการเสริมความปลอดภัยของ Cisco SD-WAN ระบุว่า อินเทอร์เน็ตสำหรับผู้ดูแลระบบ เช่น พอร์ต 443, 22 และ 830 ไม่ควรถูกเปิดให้เข้าถึงจากอินเทอร์เน็ตโดยตรง การเข้าถึง Manager ผ่าน HTTPS ควรมาจาก Jump Host หรือเครือข่ายสำหรับการจัดการระบบ (Management Subnet) เท่านั้น

การตรวจสอบสัญญาณว่าระบบถูกโจมตี

สัญญาณที่ Cisco ระบุว่าสามารถใช้ตรวจสอบการถูกโจมตีเกี่ยวข้องกับ `j_security_check` ซึ่งเป็นเส้นทางที่ Manager ใช้สำหรับการเข้าสู่ระบบผ่านเซสชัน ในตัวอย่างของ Cisco ผู้โจมตีจะเข้ารหัสอักขระหนึ่งตัวของเส้นทางดังกล่าว ทำให้กลายเป็น `/%6a_security_check` โดย `%6a` หมายถึงตัวอักษร `j`

มีไฟล์ Log 2 ตำแหน่งที่ควรตรวจสอบรายการ `j_security_check` ซึ่งมาจาก IP Address ที่ไม่รู้จักหรือไม่ได้รับอนุญาต ได้แก่

- File: `/var/log/nms/containers/service-proxy/serviceproxy-access.log`
- File: `/var/log/nms/vmanage-server.log` โดยเฉพาะรายการที่เกี่ยวข้องกับชื่อผู้ใช้ซึ่งขึ้นต้นด้วย `viptela-reserved-`

ชื่อที่ขึ้นต้นด้วย `viptela-reserved-` เป็นชื่อบัญชีระบบที่สงวนไว้สำหรับการทำงานของบริการต่างๆ

ผู้โจมตีสามารถเข้ารหัสอักขระใดก็ได้ในคำขอ ดังนั้น `%6a` จึงเป็นเพียงตัวอย่างหนึ่งเท่านั้น รายการลักษณะเดียวกันอาจเกิดขึ้นจากการทำงานปกติของระบบได้เช่นกัน จึงจำเป็นต้องตรวจสอบแต่ละรายการเทียบกับกิจกรรมปกติของระบบ เพื่อป้องกันการแจ้งเตือนผิดพลาด

หากต้องการตรวจสอบเพิ่มเติมว่า Manager ถูกโจมตีหรือถูกยึดระบบแล้วหรือไม่ ลูกค้านำสามารถเปิดเคสระดับ Severity 3 กับ Cisco TAC และระบุ CVE-2026-76504 ไว้ในหัวข้อของเคส โดย Cisco ขอให้ลูกค้ารันคำสั่ง `request admin-tech` บน Manager ก่อน เพื่อให้สามารถส่งไฟล์ผลลัพธ์ไปให้ทีม Cisco ตรวจสอบได้

ประกาศของ Cisco ไม่มี Detection Rule สำหรับตรวจจับช่องโหว่นี้โดยเฉพาะ และไม่ได้ระบุว่าการอัปเดตระบบจะลบการเข้าถึงของผู้โจมตีที่มีอยู่แล้วออกจากระบบหรือไม่

ในประกาศของ Cisco สำหรับช่องโหว่ในเดือนพฤษภาคมและช่องโหว่ตัวแรกในเดือนมิถุนายน ระบุว่า การอัปเดตเพียงอย่างเดียวไม่สามารถแก้ไขกรณีที่ระบบถูกโจมตีและถูกยึดไปแล้วได้ โดยแนะนำให้ลูกค้าเก็บไฟล์ `admin-tech` ไว้ก่อนดำเนินการอัปเดต

CVE-2026-76504 เกิดขึ้นต่อเนื่องจากช่องโหว่ใน Cisco SD-WAN หลายรายการที่ถูกพบว่ามีคนนำไปใช้โจมตีจริงในปี 2026 วันที่ 30 กันยายน 2026 รายการ Known Exploited Vulnerabilities (KEV) ของหน่วยงาน Cybersecurity and Infrastructure Security Agency (CISA) ของสหรัฐฯ ระบุว่า มีช่องโหว่ Cisco SD-WAN จำนวน 8 รายการที่ถูกเพิ่มเข้ามาในปี 2026

ข้อมูลอ้างอิง

Sep 30, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/09/cisco-warns-of-attackers-exploiting.html>