วันที่ 1 กันยายน 2568

Citrix ออกแพตช์แก้ไขช่องโหว่ด้านความปลอดภัย 3 รายการใน NetScaler ADC และ NetScaler Gateway

Citrix ได้ออกแพตช์แก้ไขช่องโหว่ด้านความปลอดภัย 3 รายการในผลิตภัณฑ์ NetScaler ADC และ NetScaler Gateway โดยหนึ่งในนั้นได้รับการยืนยันแล้วว่า มีการถูกใช้โจมตีจริงแล้วซึ่งผู้ใช้งานควรเร่งอัปเดตระบบโดยทันที

ช่องโหว่ที่ถูกแก้ไข ได้แก่:

- CVE-2025-7775 (CVSS 9.2): ช่องโหว่ Memory Overflow ที่นำไปสู่การรันโค้ดจากระยะไกล (Remote Code Execution) และ/หรือ Denial-of-Service
- CVE-2025-7776 (CVSS 8.8): ช่องโหว่ Memory Overflow ที่อาจทำให้เกิดพฤติกรรมผิดพลาดแบบไม่คาดคิด และ Denial-of-Service
- CVE-2025-8424 (CVSS 8.7): ช่องโหว่การควบคุมสิทธิ์เข้าถึงที่ผิดพลาด (Improper Access Control) บนอินเทอร์เฟซจัดการของ NetScaler

ทางบริษัทระบุว่า “พบการโจมตีช่องโหว่ CVE-2025-7775 บนอุปกรณ์ที่ยังไม่ได้อัปเดต” แต่ไม่ได้ให้รายละเอียดเพิ่มเติม

เงื่อนไขการโจมตีแต่ละช่องโหว่

การโจมตีช่องโหว่แต่ละรายการมีเงื่อนไขก่อนใช้งาน ดังนี้:

- CVE-2025-7775: NetScaler ต้องถูกตั้งค่าเป็น Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) หรือ AAA virtual server โดยมีเงื่อนไขเพิ่มเติมเฉพาะสำหรับแต่ละเวอร์ชันและประเภทของ Load Balancer ที่ผูกกับ IPv6 services หรือ DBS IPv6 services รวมถึง CR virtual server ประเภท HDX
- CVE-2025-7776: NetScaler ต้องถูกตั้งค่าเป็น Gateway โดยมี PCoIP Profile ผูกอยู่
- CVE-2025-8424: ต้องสามารถเข้าถึง NSIP, Cluster Management IP, local GSLB Site IP หรือ SNIP ที่เปิดสิทธิ์ Management Access ได้

เวอร์ชันที่ได้รับการแก้ไข

Citrix ได้แก้ไขปัญหาแล้วในเวอร์ชันต่อไปนี้ โดยไม่มีวิธีแก้ไขชั่วคราว:

- NetScaler ADC และ NetScaler Gateway: 14.1-47.48 และเวอร์ชันใหม่กว่า
- NetScaler ADC และ NetScaler Gateway: 13.1-59.22 และเวอร์ชันใหม่กว่าของ 13.1
- NetScaler ADC 13.1-FIPS และ 13.1-NDcPP: 13.1-37.241 และเวอร์ชันใหม่กว่า
- NetScaler ADC 12.1-FIPS และ 12.1-NDcPP: 12.1-55.330 และเวอร์ชันใหม่กว่า

Citrix ให้เครดิตกับ Jimi Sebree จาก Horizon3.ai, Jonathan Hetzer จาก Schramm & Partnerfor และ François Hämmerli ที่ค้นพบและรายงานช่องโหว่เหล่านี้

CVE-2025-7775 นับเป็นช่องโหว่ล่าสุดของ NetScaler ADC และ Gateway ที่ถูกนำมาใช้โจมตีจริงในระยะเวลาอันสั้น หลังจาก CVE-2025-5777 (หรือที่รู้จักในชื่อ Citrix Bleed 2) และ CVE-2025-6543

การเปิดเผยครั้งนี้เกิดขึ้นเพียงหนึ่งวัน หลังจากที่หน่วยงาน U.S. Cybersecurity and Infrastructure Security Agency (CISA) ได้เพิ่มช่องโหว่ด้านความปลอดภัยอีก 2 รายการที่กระทบกับ Citrix Session Recording (CVE-2024-8068 และ CVE-2024-8069) เข้าไปใน Known Exploited Vulnerabilities (KEV) catalog จากหลักฐานที่พบว่ามีการโจมตีใช้งานจริงแล้ว

ข้อมูลอ้างอิง

Aug 26, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/citrix-patches-three-netscaler-flaws.html