THREAT BULLETINS

Operation ZeroDisco Campaign Exploits Cisco SNMP Flaw (CVE-2025-20352)

TLP:WHITE

Oct 16, 2025

On October 15, 2025, Trend Micro disclosed an active attack campaign, dubbed Operation ZeroDisco, exploiting two vulnerabilities in older, unpatched Cisco devices. The primary flaw being exploited in the campaign, tracked as CVE-2025-20352, is a critical simple network management protocol (SNMP) vulnerability. Conversely, the other flaw is a modified Telnet flaw, identified as CVE-2017-3881.

The campaign enables authenticated remote code execution (RCE) to deploy a Linux rootkit that grants attackers persistent, stealthy access to network infrastructure. A vendor patch is available for CVE-2025-20352, and patching and mitigation are recommended to prevent core network compromise.

Health-ISAC is sharing this to increase situational awareness and encourage organizations to assess their level of risk to this activity.

Analysis

Operation ZeroDisco primarily leverages a stack overflow vulnerability in the Cisco Simple Network Management Protocol (SNMP) subsystem, tracked as CVE-2025-20352. This flaw affects

Cisco IOS and IOS XE software in which an authenticated attacker can exploit the vulnerability by sending specially crafted SNMP packets to an affected device. A denial-of-service (DoS) condition can be triggered by an attacker with low privileges leveraging the SNMPv2c or earlier read-only community string or valid SNMPv3 user credentials. An attacker with high privileges can execute code as the root user, leveraging the SNMPv1 or v2c read-only community string or valid SNMPv3 user credentials and administrative or privilege 15 credentials on an affected device. The campaign also exploits a modified Telnet vulnerability based on CVE-2017-3881 to enable memory read/write access at arbitrary addresses.

The threat actors were observed targeting multiple devices, including Cisco 9400 and 9300 series switches and legacy 3750G series devices. Additionally, Operation ZeroDisco utilized different exploitation techniques based on the target system's architecture. On older 32-bit systems, the attackers relied on malicious SNMP packets to send initial commands, which were often chained with a modified Telnet exploit to achieve memory read/write access at arbitrary addresses. Conversely, against 64-bit switch builds, the core SNMP exploit was used to deploy the Linux rootkit directly onto the device. Following deployment, the attackers leveraged the rootkit's universal password feature to gain privileged access, where they then established a fileless backdoor for persistence.

The rootkit establishes persistent, covert control over the critical network infrastructure. Its key functions include acting as a UDP listener on any port for command-and-control (C2) without the port being explicitly open, bypassing VTY access control lists (ACLs) to ensure remote access, hiding specific account names or EEM scripts from the running configuration to maintain stealth, and resetting the last running-config write timestamp to conceal changes from administrators. By compromising core switches, the attackers can conduct lateral movement, traffic monitoring, and command execution activity deep within the network.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Applying the patch for CVE-2025-20352 provided in updated software releases from Cisco patch
- Leveraging Cisco's software checker to determine exposure to vulnerabilities.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	thehackernews, hhs, trendmicro, bleepingcomputer, cisco, cyware, infosecurity-magazine, cisco 1, securityweek

Alert ID d978698f

View Alert

Share Feedback

was this helpful? |

Tags Operation ZeroDisco, CVE-2017-3881, CVE-2025-20352, Cisco IOS, Cisco IOS XE, Trend Micro

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**