

Weekly Intelligence Summary

Report Date: 02.03.2026

Intelligence Cut-off Date: 27.02.2026

Weekly Focus: Cisco SD-WAN Zero-Day

A critical Zero Day in Cisco Catalyst SD-WAN devices, actively exploited since 2023, allows threat actors to bypass authentication and gain administrative access.

Campaigns targeting Cisco Catalyst SD-WAN Controllers and Managers have reportedly been active since at least 2023, leveraging a critical Zero Day tracked as CVE-2026-20127 (OVSS: 77 | CVSS: 10). The vulnerability enables authentication bypass, granting non-root administrative privileges and access to the Network Configuration Protocol (NETCONF) to manipulate SD-WAN network configurations.

In exploitation, UAT-8616 registered rogue peers with the Cisco SD-Wan Management and control plane, gaining trusted access to critical devices. Privilege escalation was achieved by downgrading vSmart controllers to versions vulnerable to CVE-2022-20775 (OVSS: 74 | CVSS: 7.8), providing root-level access. This allowed threat actors to establish persistence via SSH authorised keys, local account manipulation, and startup script modification. Interactive access was maintained by re-exploiting CVE-2026-20127.

Lateral movement within affected SD-WAN environments leveraged NETCONF over port 830 and SSH. Detection evasion was achieved by clearing system logs and shell history, removing Elasticsearch database indicators, and disabling network interfaces used for external logging. No malware was detected, indicating a reliance on native infrastructure.

Why It Matters...

Despite no specific attribution to a particular nation state, the threat actor UAT-8616 demonstrates capabilities aligned with a highly sophisticated threat actor, which Orpheus assess as highly likely to be associated with a nation state threat actor, in part due to historic reporting of state-sponsored threat actors targeting public-facing infrastructure, specifically Cisco appliances.

The discovery of this 0-day vulnerability after 3 years (with exploitation evidence dating back to 2023) highlights the persistent nature of UAT-8616, and follows a consistent trend throughout recent years of edge devices being targeted to establish persistent footholds into organisations for subsequent post-exploitation activity.

Organisations using the products affected by CVE-2026-20127 are strongly advised to follow security advisories relating to this vulnerability, alongside the Cisco Catalyst SD-WAN threat hunting guide released by global intelligence partners for identifying activity associated with UAT-8616's exploitation of this vulnerability.

Intelligence Overview

Ransomware

The University of Mississippi Medical Center cancelled its appointments and closed all clinics statewide following a ransomware incident that likely resulted from a supply chain compromise of Epic electronic medical record software.

OAPT, the alleged new ransomware-as-a-service operation that claimed 70+ victims from 28 January to 2 February, including Urban Outfitters, has been assessed as unreliable, as many of its victims appear to be fabricated, unverifiable, or recycled.

Nation-State

Since at least mid-2024, China-linked UNC6201 has been exploiting a critical zero-day in Dell RecoverPoint for VM, tracked as CVE-2026-22769 (OVSS: 77 | CVSS: 10).

UAT-10027, which is linked to the North Korea-aligned Lazarus Group with low confidence, is targeting US education and healthcare entities with the novel 'Dohdoor' backdoor since at least December 2025.

Exploits

An active ClickFix campaign is compromising legitimate websites to deploy the custom MIMICRAT in a multi-stage infection chain.

From December 2025 to February 2026, a Russian-speaking financially motivated threat actor leveraged multiple commercial AI services to compromise 600+ FortiGate devices across 55 countries. The adversary exploited exposed management ports and weak credentials without MFA, rather than vulnerabilities.