

Weekly Intelligence Summary

Report Date: 06.10.2025

Intelligence Cut-off Date: 03.10.2025

Weekly Focus: Recently disclosed Cisco vulnerabilities exploited by state-sponsored threat actors to deliver updated malware.

The China-affiliated Storm-1849 was associated with a vulnerability exploitation campaign, leveraging Cisco Adaptive Security Appliance (ASA) vulnerabilities to deliver RayInitiator and LINE VIPER malware.

Storm-1849 was observed exploiting two Cisco Secure Firewall ASA vulnerabilities tracked as [CVE-2025-20362](#) (CVSS: 6.5 | OVSS: 83) and [CVE-2025-20333](#) (CVSS: 9.9 | OVSS: 83) to bypass authentication and execute malicious code on susceptible appliances. A third vulnerability, tracked as [CVE-2025-20363](#) (CVSS: 9 | OVSS: 65), was addressed; however, there is no evidence that the vulnerability has been exploited in the wild.

RayInitiator is a persistent multi-stage bootkit that facilitates the deployment of LINE VIPER, a user-mode shellcode loader, to Cisco ASA 5500-X series devices. In some instances, the threat actor modified the Read-Only Memory Monitor (ROMMON) to facilitate persistence across reboots and software upgrades.

Compromised devices concerned Cisco ASA 5500-X Series models 5512-X, 5515-X, 5585-X, 5525-X, 5545-X, and 5555-X that are running Cisco ASA Software releases 9.12 or 9.14 with VPN web services enabled, which do not support Secure Boot and Trust Anchor technologies.

As of 29 September 2025, 48,000 internet-exposed Cisco ASA and Firewall Threat Defence (FTD) instances were reportedly still vulnerable to [CVE-2025-20333](#) and [CVE-2025-20362](#), with most IPs located in the US, UK, Japan, Germany, and Russia.

Why It Matters...

The campaign appears to be the continuation of a series of intelligence-gathering campaigns targeting government agencies in May 2025, known as [ArcaneDoor](#). However, the use of RayInitiator and LINE VIPER payloads indicates elevated sophistication compared to the previous campaign.

Internet-facing systems continue to be targeted by threat actors as they typically occupy critical network segments, enabling lateral movement and the monitoring of network communications. They are therefore particularly attractive to state-sponsored threat actors, as was previously seen with [Salt Typhoon](#)-led targeting.

Considering the high number of instances that remain vulnerable and have reached end-of-support (EoS) status, they must be promptly upgraded or migrated to supported hardware and software.

Intelligence Overview

Third Party

Mercedes-Benz, AT&T, and AstraZeneca have been affected by a [data breach following the compromise of Credera](#). Attributed to the group 888, the breach resulted in the exposure of sensitive internal information belonging to both Credera and its clients.

A [threat actor, Grep, has claimed responsibility for breaching multiple organisations](#), including McDonald's, following a security incident involving a third-party provider. A total of 220 million records were reportedly compromised.

Harrods has disclosed a [data breach that has compromised 430,000 records](#) containing sensitive customer information.

Targeted Extortion

On 19 August 2025, [Motility Software Solutions was compromised by a ransomware incident](#). The incident exposed the PII of 766,000 customers, which may include full names, email addresses, date of birth, Social Security Numbers (SSN) and driving licence numbers.

CI0p ransomware is attempting to [extort executives with claims of stealing data from Oracle's E-Business Suite](#). In one case, the group demanded up to USD 50 million. Victims have received screenshots and file trees as proof of compromise.

Scattered Spider

WestJet has confirmed that the incident involving [Scattered Spider exposed personal information belonging to around 1.2 million individuals](#). The stolen data includes names, addresses, dates of birth, and government-issued identification details.