NCSC warns of persistent malware campaign targeting Cisco devices

Latest malware analysis report helps organisations detect and mitigate malicious activity targeting certain Cisco devices.

Today (Thursday), the National Cyber Security Centre (NCSC) – a part of GCHQ – has issued further advice to help network defenders mitigate malicious targeting of certain Cisco devices.

In a significant update on a previous malicious campaign exposed last year, Cisco has said the same threat actor has exploited new vulnerabilities in Cisco Adaptive Security Appliance (ASA) 5500-X Series devices to implant malware, execute commands, and potentially exfiltrate data from compromised devices.

The NCSC is calling on network defenders using affected products to urgently investigate this activity and has published new analysis of the malware components – dubbed RayInitiator and LINE VIPER – to assist with detection and mitigation.

Organisations are urged to follow Cisco's recommended remediation advice, including applying security updates, and to report any evidence of compromise to the NCSC.

As some Cisco ASA 5500-X series models will be out of support from September 2025 and August 2026, the NCSC strongly recommends, where practicable, such devices should be replaced or upgraded. Obsolete and end-of-life devices present a significant security risk to organisations.

NCSC Chief Technology Officer, Ollie Whitehouse said:

> *"It is critical for organisations to take note of the recommended actions highlighted by Cisco today, particularly on detection and remediation.*
>
> *"We strongly encourage network defenders to follow vendor best practices and engage with the NCSC's malware analysis report to assist with their*

investigations.

"End-of-life technology presents a significant risk for organisations. Systems and devices should be promptly migrated to modern versions to address vulnerabilities and strengthen resilience."

The alert follows a joint advisory published last year with international partners, which included detailed analysis of malware, dubbed LINE DANCER and LINE RUNNER.

The RayInitiator and LINE VIPER malware represents a significant evolution on that used in the previous campaign, both in sophistication and its ability to evade detection. More information on managing obsolete and end of life devices can be found in the device security guidance.

The NCSC recently published a blog highlighting that organisations should prepare for Windows 10 coming to end of life in October and prioritise migration to Windows 11.

Cisco has provided further information and detection advice available on their website: https://sec.cloudapps.cisco.com/security/center/resources/detection_guide_for_continued_attacks

PUBLISHED

25 September 2025

WRITTEN FOR

Large organisations

Cyber security professionals

Public sector

NEWS TYPE

Alert