

CISCO FIREWALLS HIT BY ZERO-DAY EXPLOITS

A global espionage campaign is exploiting zero-day flaws in Cisco ASA and FTD firewalls. US agencies have been forced into emergency response mode-and enterprises worldwide are now exposed.



One

Three Zero-Days, Two Already Exploited



- *CVE-2025-20333: Remote Code Execution (actively exploited)*
- *CVE-2025-20362: VPN Web Access bypass (actively exploited)*
- *CVE-2025-20363: Web services RCE (not yet seen in the wild)*

Together, these flaws strike at the trust anchor of the enterprise perimeter - the firewall.



Two

Hackers Didn't Just Break In - They Embedded Themselves



Attackers disabled firewall logging, intercepted CLI commands, tampered with boot ROM, and deployed custom malware implants (RayInitiator, Line Viper). These techniques guarantee persistence - even after reboots or firmware upgrades.



Three

CISA Issues Emergency Directive 25-03

*The US government called this an
"unacceptable risk."*



Agencies must:

- *Identify every Cisco firewall in use*
- *Collect memory dumps and forensics*
- *Isolate or replace compromised hardware*
- *Report status within strict deadlines*

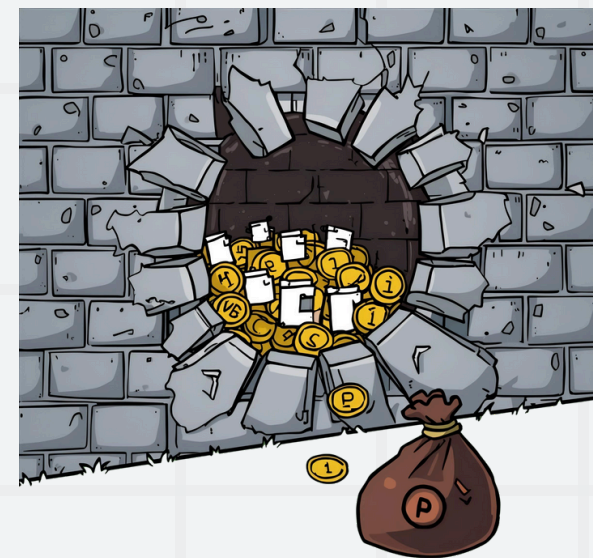
*This is no routine patch cycle - it's a national
emergency.*

www.getastra.com 



Four

When the Firewall Falls, Everything Inside Is Exposed



Compromised firewalls enable attackers to silently:

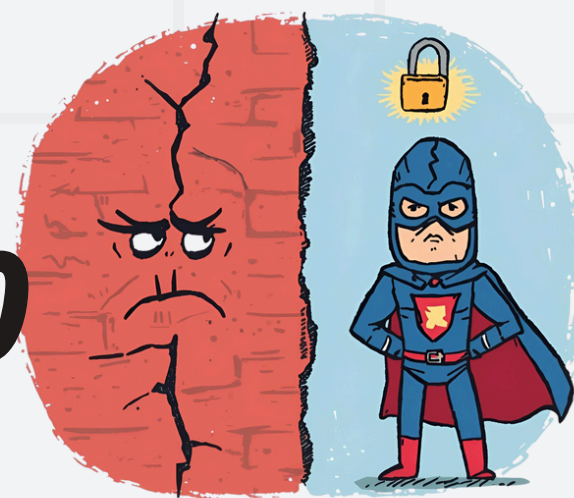
- *Monitor enterprise traffic*
- *Reroute or alter data*
- *Exfiltrate sensitive IP and customer records*

With many Cisco ASA models already end-of-life, leaders must face a hard truth: no patch may be coming.



Five

Immediate Action Required - No Time to Wait



From Compromized + Secured.

Act now to secure your perimeter:

- *Map every Cisco ASA and FTD deployment across your environment.*
- *Apply available patches immediately to supported models.*
- *Decommission or replace end-of-life hardware that will never receive fixes.*
- *Run full forensic analysis to detect implants or tampering at the boot level.*
- *Rotate all keys, certificates, and credentials to cut off hidden access.*
- *Restrict management interfaces so only trusted, internal networks can reach them.*

www.getastra.com 

