It's Probably Nothing
by Sierra Echo Charlie

EDITION 17 / 30 OCTOBER 2026

# Cisco’s VPN flaw can restart the firewall

Plus PHP2Shell’s kernel-level follow-up and two distinct Juniper compromise paths.

3 stories / Listen online - 3:30

01 / THE BRIEF

## No successful login needed for this firewall restart

Cisco says CVE-2026-76418 is being actively exploited. A crafted connection request can make a vulnerable ASA or FTD appliance reload, but the configuration matters: exposure requires a reachable SSL remote-access VPN service with secondary authentication in an applicable tunnel group. The attacker doesn’t need a successful VPN login.

There’s an awkward configuration detail, too: removing the tunnel-group list doesn’t remove exposure if DefaultWEBVPNGroup still uses secondary authentication. Removing a menu isn’t the same as removing the vulnerable path.

The disclosed impact is denial of service, not code execution or data theft. Cisco says it became aware of exploitation during October, without naming attackers, victims or the scale.

WORTH ASKING

If you’re running this configuration, Cisco’s branch-specific fix table is worth checking. Fixes are available; the configuration-dependent mitigations can alter VPN functionality or weaken authentication, so they’re not an equivalent substitute.

SOURCES

Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Tunnel Denial of Service Vulnerability - Primary source

CVE-2026-76418 - Cisco CNA record - Primary source

Exploited Cisco ASA and FTD SSL VPN Flaw Enables Remote Device Restarts - Reporting / context

02 / THE BRIEF

# PHP2Shell's root stage joins the known-exploited list

CISA has added Linux kernel CVE-2026-46300 to its known-exploited catalogue, explicitly linking it to PHP2Shell chains that implant webshells and run commands as root. This isn't another notice about the two PHP bugs: the newly listed component is the privilege-escalation stage.

For context, Dream's 26 October report attributed 24 compromised perimeter firewalls and one internal firewall-management server to the chain. In its recovered implementation, the PHP stage ran as nobody; Fragnesia then modified page-cache-backed PAM configuration to permit root access. Dream withheld the vendor and affected versions, so those findings don't identify a particular firewall product.

CISA's new entry requires forensic triage and sets a 31 October remediation deadline for covered federal agencies. The question extends beyond whether PHP is patched to whether the appliance was rooted.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

CISA Adds Two Known Exploited Vulnerabilities to Catalog - Primary source

Chained PHP2Shell Exploit Roots 25 Servers, including US Government Servers - Primary source

PHP2Shell Exploitation Prompts CISA Deadline as Researchers Report Firewall Compromises - Reporting / context

03 / THE BRIEF

# Juniper's two root paths have different boundaries

Juniper says CVE-2026-103406 lets an unauthenticated remote attacker execute commands as root on Session Smart Conductor through a specially crafted salt minion ID handled by AutomatedProvisioner.

A second flaw, CVE-2026-103409, allows unauthenticated administrative access through crafted URL parameters on Session Smart Router-but only before the device is onboarded to Mist or Conductor. That's a meaningful restriction, not a footnote: it doesn't describe exposure across an already-onboarded router fleet.

The corresponding fixed releases are 7.0.5, 7.1.7 and 7.2.3. Juniper lists no workaround for either flaw and says it isn't aware of malicious exploitation. The Conductor root-command path is substantial enough without borrowing urgency from attacks the vendor hasn't reported.

SOURCES

CVE-2026-103406 - Juniper CNA record - Primary source

CVE-2026-103409 - Juniper CNA record - Primary source

Juniper Fixes Ten Vulnerabilities in Session Smart Router and Conductor - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.