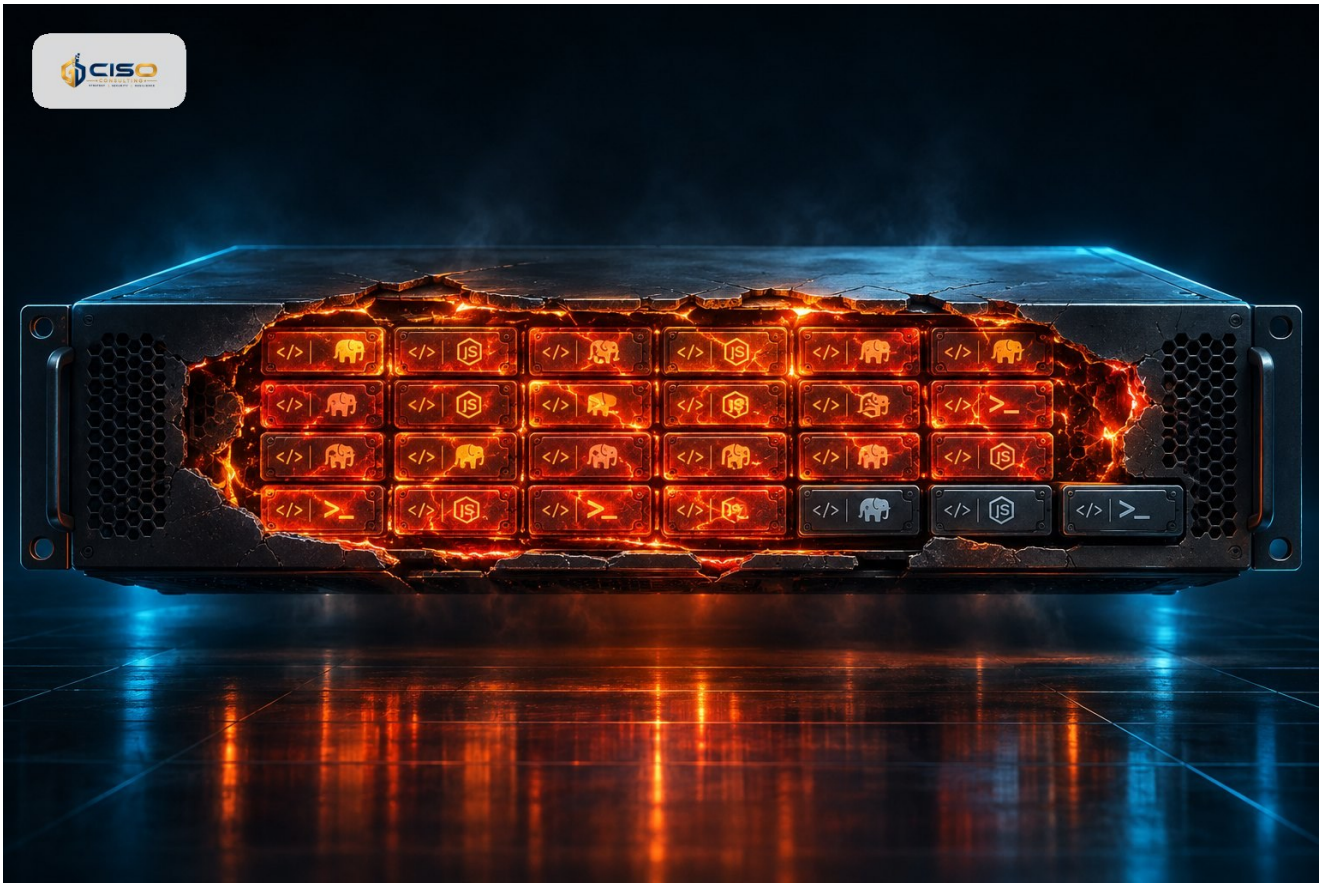
InfraTrust: Most exploited appliance flaws now sit in bundled third-party components



Eclypsium's November InfraTrust report finds that 33 of 38 advisories covering exploited flaws involved bundled components such as PHP, Node.js and OpenSSH. It lists priority patches and advises hardening before fixes arrive.

- The report covers 373 advisories from 23 infrastructure vendors between October 15 and November 19, with 3,880 vulnerabilities; 98 advisories were rated critical.
- 38 advisories included flaws in CISA's KEV catalog, and 33 of them concerned bundled components, mainly PHP, Node.js and OpenSSH.
- PHP2Shell (CVE-2026-109618 and CVE-2026-109619) is being exploited against Palo Alto Networks and Check Point firewalls; fixes for several other vendors were partial or missing as of November 20.

> - Priority items include Cisco Expressway, Check Point gateways, Arista VeloCloud Orchestrator, Cisco ASA and FTD, and SonicWall SonicOS.
> - InfraTrust advises removing management interfaces from the Internet, segmenting them, and checking previously exposed devices for backdoors.

Eclypsium's November InfraTrust Pulse report suggests that exposure to exploited vulnerabilities in network appliances increasingly depends on software the vendors did not write themselves.

What the report found

Between October 15 and November 19, the report tracked 373 advisories from 23 infrastructure vendors. Of the 38 advisories that included vulnerabilities in CISA's KEV catalog, 33 fixed flaws in bundled components, primarily PHP, Node.js and OpenSSH. Even after an upstream fix is released, customers must wait until each vendor rebuilds its product.

The PHP2Shell flaws (CVE-2026-109618 and CVE-2026-109619) illustrate the problem. They are being exploited against Palo Alto Networks and Check Point firewalls, chained with other flaws to obtain root access. Check Point reported destructive attacks that deployed data-wiping malware on VMware ESXi hosts. As of November 20, fixes for Fortinet, Juniper, Lenovo, HPE, Netgear, HP and Siemens products were partial or not yet released.

Patches to prioritize

InfraTrust points to Cisco Expressway (CVE-2026-76466), the PHP2Shell flaws and CVE-2026-123039 in Check Point gateways, Arista VeloCloud Orchestrator (CVE-2026-114625), Cisco Secure Firewall ASA and FTD (CVE-2026-76418) and SonicWall SonicOS (CVE-2026-19868). It also recommends Fortinet's October hardening updates.

Before and after the patch

Because fixes can lag, the report advises taking management interfaces off the Internet, segmenting them internally to limit lateral movement, and investigating previously exposed devices, since backdoors can survive patching.

What to do now

1. Check your firewall, VPN and gateway inventory against the products and CVEs listed and patch the exploited ones first.
2. Ask each appliance vendor for the status of PHP2Shell, PHP, Node.js and OpenSSH fixes, and record the answers.
3. Remove device management interfaces from Internet exposure and restrict them to segmented

administrative networks.

4. Review devices that were previously exposed for signs of backdoors or persistence, even if already patched.
5. Include bundled third-party components and vendor rebuild timelines in third-party risk and vulnerability management reviews.