



The one thing that matters in cybersecurity this week — and what to do about it.

Provided by Major Business Solutions LLC

HEADLINE THREAT

ACTIVE ADVISORY · #STOPRANSOMWARE

SafePay ransomware has hit 600+ organizations by breaking in through firewalls and VPNs — then wiping the backups

On October 20, CISA, the FBI, the U.S. Secret Service and German and UK partners issued a joint advisory (AA26-293A) on the SafePay ransomware group, active since August 2024. SafePay gets in through stolen or brute-forced passwords and through known, already-patched flaws in **SonicWall firewalls, Cisco ASA/Firepower VPNs and Veeam Backup & Replication**. Once inside, operators use everyday admin tools (RDP, PsExec, AnyDesk, TeamViewer), steal data, and then stop shadow copies and **factory-reset the network storage holding backups** — in some cases deleting every network-attached backup before demanding a ransom.

Why it matters for you

This is a playbook aimed squarely at small and mid-size businesses: the doors are the firewall, VPN and backup software most SMBs run, and the bugs involved have had fixes for one to six years. If a backup can be reached from your network with an admin password, assume an attacker can erase it. The good news: patching, MFA on remote access and one offline backup copy defeat most of this attack.

PATCH PRIORITY

SafePay **Firewall/VPN** **SonicWall SonicOS — CVE-2024-40766** and **Cisco ASA/FTD — CVE-2020-3259, CVE-2023-20269**. Named in the SafePay advisory as entry points. Update firmware and require MFA on all VPN logins.

SafePay **Backup** **Veeam Backup & Replication — CVE-2023-27532, CVE-2024-40711**. Exploited to reach and destroy backups. Update Veeam and keep its server off the internet.

KEV **Firewall** **Fortinet FortiOS — CVE-2025-61624**. Added to CISA's exploited list this month; used to plant the PEERSTITCH implant on 500+ FortiGate firewalls.

KEV **Remote access** **BeyondTrust Remote Support — CVE-2026-102764**. Authentication bypass exploited since late August; cloud customers were patched Oct 8, self-hosted appliances must be patched manually and reviewed.

Websites **PHP "PHP2Shell" — CVE-2026-109618, CVE-2026-109619** (CVSS 9.2). Emergency PHP fixes released Oct 21 (8.5.12 / 8.4.27 / 8.3.36 / 8.2.35); exploit attempts already observed. Affects most PHP-based sites, including WordPress — updating WordPress alone does not fix it.

BY THE NUMBERS

600+

organizations hit by
SafePay since Aug 2024

CISA/FBI AA26-293A, Oct
2026

31%

of breaches began with
an exploited vulnerability
— now the #1 way in

Verizon 2026 DBIR, May
2026

48%

of breaches involved
ransomware

Verizon 2026 DBIR, May
2026

\$3B+

lost to business email
compromise in 2025

FBI IC3 2025 report, Apr
2026

THREE ACTIONS THIS WEEK

- 1. Patch the front door.** Ask your IT provider to confirm, in writing, that your firewall/VPN (SonicWall, Cisco, Fortinet) and Veeam are on current versions, and that every VPN and remote-access login requires MFA. Retire any old or unused VPN accounts.
- 2. Make one backup they can't reach.** Keep at least one copy offline or immutable (cloud object-lock or rotated drives), use separate credentials for the backup system that are not tied to your normal admin accounts, and do a test restore of one critical file share.
- 3. Check your website and remote-support tools.** Ask your web host to confirm PHP has been updated for PHP2Shell, and review who can use AnyDesk, TeamViewer or BeyondTrust on your network — remove anything you don't recognize.



Provided by Major Business Solutions LLC

Sources

- [CISA — #StopRansomware: SafePay Ransomware \(AA26-293A\)](#)
- [FBI IC3 — #StopRansomware: SafePay Ransomware \(PDF\)](#)
- [CISA — Adds Six Known Exploited Vulnerabilities to Catalog \(Oct 20\)](#)
- [SC Media — CISA adds Fortinet and BeyondTrust flaws to exploited list](#)
- [BleepingComputer — BeyondTrust patches zero-day exploited since August](#)
- [The Hacker News — PHP issues emergency patches for PHP2Shell RCE flaws](#)
- [The Hacker News — CISA orders agencies to patch Plex2Shell, Siemens, SiteGuard flaws](#)
- [TechRepublic — Verizon 2026 DBIR: vulnerability exploitation leads](#)
- [The Record — FBI IC3 2025 report: cyber fraud surges](#)

Always verify advisories and patch guidance directly with CISA (cisa.gov) and your vendors before acting. This briefing is a summary, not a substitute for vendor instructions.