



The one threat that matters this week, and what to do about it — in five minutes.

Provided by Major Business Solutions LLC

HEADLINE THREAT ACTIVE ADVISORY

#StopRansomware: SafePay gang has hit 600+ organizations through VPNs, firewalls and backup servers

On October 20, CISA, the FBI, the U.S. Secret Service and German and UK partners published joint advisory **AA26-293A** on SafePay ransomware. The group has hit at least 600 organizations since August 2024. It gets in with stolen or brute-forced credentials, phishing, and known flaws in **Cisco ASA/FTD VPNs, SonicWall firewalls** and **Veeam Backup & Replication**. Once inside, SafePay uses ordinary admin tools (RDP, PsExec, AnyDesk, TeamViewer) to move around, copies data out to cloud storage, then **stops shadow copies and resets backup NAS devices to factory settings** before encrypting. Victims then get phone calls threatening to leak their data.

Why it matters for you: The tools SafePay goes after are the ones most small businesses run: a SonicWall or Cisco firewall/VPN, Veeam for backups, a NAS for storage, and AnyDesk or TeamViewer for IT support. The bugs it exploits have been patched for one to five years, so the businesses getting hit are mostly the ones that never applied the updates. If your backups sit on the same network with the same admin passwords, plan on losing them along with everything else.

PATCH PRIORITY

Firewall **SafePay** **SonicWall SonicOS — CVE-2024-40766.** Improper access control in management/SSL-VPN. Update firmware, reset local passwords, enforce MFA on SSL-VPN.

VPN **SafePay** **Cisco ASA / FTD — CVE-2020-3259, CVE-2023-20269.** Lets attackers brute-force VPN logins and leak memory contents. Patch, and turn on MFA and lockout for remote access.

Backup **SafePay** **Veeam Backup & Replication — CVE-2023-27532, CVE-2024-40711 (CVSS 9.8).** Leaks credentials and allows unauthenticated code execution. Update to a current build and keep the backup server off the domain.

Firewall **KEV Oct 16** **Fortinet FortiOS and other products — CVE-2025-61624.** Path traversal that the PEERSTITCH malware has used to backdoor 500+ firewalls. Patch, and check for unfamiliar auto-scripts.

Remote access **KEV Oct 16** **BeyondTrust Remote Support — CVE-2026-102764.** Authentication bypass, actively exploited. Matters most if your MSP uses it to support you. Ask them to confirm they've patched.

Firewall **KEV Oct 14** **Palo Alto PAN-OS — CVE-2026-0322.** Code execution in the management interface. Patch, and allow management access only from trusted internal IPs.

Backup **KEV Oct 14** **Ahsay AhsayCBS — CVE-2026-105133 / -105134.** Chained to plant webshells. Earlier patches were incomplete, so apply v10.3.4.45 or v9.15.2.70 and reboot.

Website **Supply chain** **WordPress Rank Math PRO 3.0.123.** Copies downloaded Oct 15–16 carried a backdoor. If it was ever activated, treat the site as compromised: restore from a clean backup and rotate all keys. Updating alone does not remove it.

BY THE NUMBERS

600+

organizations hit by
SafePay since Aug 2024

CISA/FBI AA26-293A, Oct
2026

96%

of ransomware victims
were small organizations

Verizon 2026 DBIR

38% / 29%

of victims breached via
stolen credentials /
unpatched edge devices

Verizon 2026 DBIR

\$4.99M

global average cost of a
data breach (record high)

IBM Cost of a Data Breach
2026

THREE ACTIONS THIS WEEK

1. **Patch and lock down the front door.** Have IT or your MSP confirm in writing that your firewall/VPN (SonicWall, Cisco, Fortinet, Palo Alto) runs current firmware, that its management page can't be reached from the internet, and that every VPN login requires MFA.
2. **Get one backup the attackers can't reach.** Update Veeam or Ahsay, keep at least one copy offline or immutable (with separate credentials, not on the domain), and do a test restore of one critical system this week.
3. **Review who has remote access.** List every AnyDesk, TeamViewer and BeyondTrust install and every admin account. Remove anything you don't recognize, and ask your MSP which remote-support tools they use on your systems and when they last patched them.



Provided by Major Business Solutions LLC

Sources

1. [CISA — #StopRansomware: SafePay Ransomware \(AA26-293A\), Oct 20, 2026](#)
2. [GBHackers — CISA warns SafePay has hit 600+ organizations and destroyed backup systems](#)
3. [CISA — Adds Six Known Exploited Vulnerabilities to Catalog, Oct 20, 2026](#)
4. [CISA — Adds Two Known Exploited Vulnerabilities to Catalog, Oct 16, 2026](#)
5. [SC Media — CISA adds Fortinet and BeyondTrust vulnerabilities to exploited list](#)
6. [Help Net Security — CISA flags exploited flaws in Palo Alto, Cisco and Ahsay products](#)
7. [BleepingComputer — WordPress SEO plugin Rank Math compromised to backdoor websites](#)
8. [CISA — Known Exploited Vulnerabilities Catalog](#)
9. [Cyber Readiness Institute — 2026 DBIR: small businesses face escalating cyber threats \(Jun 2026\)](#)
10. [eSecurity Planet — IBM 2026 Cost of a Data Breach Report key findings \(Jul 2026\)](#)

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