

**FOR IMMEDIATE RELEASE**

October 22, 2026

## **Limehawk Urges Businesses to Lock Down Edge Devices After SafePay Ransomware Advisory**

*The FBI, CISA and partner agencies say SafePay gets in through stolen or guessed passwords, VPN access and known vulnerabilities, then goes after backups and recovery tools before encrypting files.*

KNOXVILLE, Tenn., Oct. 22, 2026. Limehawk, LLC, a Knoxville managed IT services provider, today urged businesses to patch firewalls and other edge devices, require multifactor authentication and protect their backups after U.S., German and U.K. agencies warned about the SafePay ransomware group.

The joint advisory, AA26-293A, was released Oct. 20, 2026 by the FBI, CISA, the U.S. Secret Service, Germany's Landeskriminalamt Rheinland-Pfalz, the U.K.'s National Crime Agency and the U.K.'s North West Regional Organised Crime Unit. The agencies say SafePay "was among the most active ransomware groups in 2026" and has "impacted at least 600 separate victims from multiple critical infrastructure sectors."

### **How do SafePay attackers get in?**

According to the advisory, the FBI, the Secret Service and cybersecurity researchers observed SafePay actors gaining initial access through credential exposure, brute force password attacks and exploiting VPN access. The advisory says the actors use IP addresses of the VPN provider Mullvad and phished account profiles to exploit CVE-2020-3259 and CVE-2023-20269 in edge device products. The agencies also observed them using automated scripts to exploit CVE-2023-27532, CVE-2024-40711 and CVE-2024-40766 on internet-exposed systems.

### **What do they do once inside?**

The advisory says SafePay actors gain administrative privileges on existing or newly created accounts, run commands on remote systems with tools such as PsExec and WinRM, and move laterally with remote management software and Remote Desktop Protocol. The agencies say the actors commonly disable security software, and in some cases changed users' passwords so valid logins stopped working.

Before encrypting, the advisory says, the actors exfiltrate data with tools including WinSCP, RClone and OneDrive, halt the Volume Shadow Copy Service, and reset network attached storage holding backups to factory settings. Encrypted files end in .SafePay, and the agencies say that data "cannot be recovered without the decryption key." If a victim does not pay, SafePay posts the stolen data to its leak site.

## What should businesses do?

Limehawk recommends these steps:

- **Patch edge devices first.** The advisory's key actions start with patching systems, "especially firewalls, and other edge devices," and its mitigations say to prioritize known exploited vulnerabilities in internet-facing systems. Check whether any of the five CVEs above apply to your equipment.
- **Require MFA.** The agencies say to require MFA for all services to the greatest extent possible, "particularly for webmail, VPNs, and accounts that access critical systems."
- **Tighten passwords.** The advisory recommends passwords of at least 15 characters, no password reuse, and account lockouts after multiple failed login attempts.
- **Protect backups.** Keep offline backups, test restores regularly, and make sure backup data is encrypted and immutable.
- **Limit admin access.** Audit administrative accounts, apply least privilege, and restrict command-line and scripting activity.
- **Block untrusted remote access.** Keep unknown or untrusted origins from reaching remote services on internal systems, disable unused ports, and review systems for new or unrecognized accounts.
- **Segment and monitor.** Segment networks to limit lateral movement, and use network monitoring and EDR tools to spot abnormal activity.

## What if you find signs of SafePay?

The advisory lists IP addresses, file names, hashes and hostnames as indicators, and says to verify them before blocking. If a compromise is found before files are encrypted, the agencies say to isolate affected hosts, hunt to scope the intrusion, report it to the FBI or CISA, and apply eviction countermeasures. The agencies do not encourage paying a ransom.

## Sources

1. CISA, "#StopRansomware: SafePay Ransomware." Joint Cybersecurity Advisory AA26-293A, Oct. 20, 2026.  
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a>
2. CISA, "#StopRansomware: SafePay Ransomware." PDF version of AA26-293A, Oct. 20, 2026.  
[https://www.cisa.gov/sites/default/files/2026-10/aa26-293a-stopransomware-safepay-ransomware-508c\\_0.pdf](https://www.cisa.gov/sites/default/files/2026-10/aa26-293a-stopransomware-safepay-ransomware-508c_0.pdf)

## Media Contact

Corey Watson, Managing Member  
Limehawk, LLC  
[press@limehawk.io](mailto:press@limehawk.io)  
<https://limehawk.io>

###