

CISA Advisory on SafePay Ransomware: What Regulated Institutions Should Check



CISA has published a #StopRansomware advisory on the SafePay group, active since August 2024 against businesses and critical infrastructure. It describes how the group gains access, spreads and encrypts data, and urges organisations to apply recommended protections.

- SafePay has been highly active since August 2024, targeting businesses and critical infrastructure in North America, South America, Europe and Australia.
- Initial access comes from stolen or guessed passwords, exploited vulnerabilities in security systems, and phishing.
- Attackers create or take over accounts, use legitimate system tools to move around, and disable security protections.
- Files are encrypted and a ransom note demands payment in cryptocurrency.

- The advisory lists affected products, including CVE-2020-3259 and CVE-2023-20269.

CISA has released a #StopRansomware advisory describing recent activity by the SafePay ransomware group. According to the advisory, the group has been highly active since August 2024 and has targeted businesses and critical infrastructure in North America, South America, Europe and Australia. The source does not mention targeting in Saudi Arabia, but the techniques described are common to many environments.

How the attacks unfold

SafePay actors typically enter a network by stealing or guessing passwords, exploiting vulnerabilities in security systems, or using phishing. Once inside, they establish control by creating new accounts or taking over existing ones. They then use legitimate system tools to move through the network, locate valuable files and disable security protections to avoid detection.

The final stage is encryption of the victim's files, followed by a ransom note demanding payment in cryptocurrency.

Vulnerabilities referenced

The advisory's affected-products section lists CVE-2020-3259 (exposure of sensitive information to an unauthorized actor) and CVE-2023-20269, among others. The full list is in the CISA publication and should be checked against your own asset inventory.

Why it matters

None of the entry methods is exotic: credentials, unpatched security products and phishing. Institutions can reduce exposure by reviewing these basics, and by confirming that account creation and security-tool changes are monitored. CISA urges organisations to follow the mitigations in the advisory.

What to do now

1. Compare the CVEs listed in the CISA advisory with your asset and product inventory and prioritise patching of any matches.
2. Review password policies and enforce multi-factor authentication, especially on remote access and privileged accounts.
3. Alert on creation of new accounts and on changes to existing privileged accounts.
4. Monitor for disabling or tampering with security tools, and for unusual use of legitimate administrative tools.
5. Reinforce phishing awareness and test that offline, restorable backups and your ransomware response plan work.