ALERT

CISA Releases Malware Analysis Report on RESURGE Malware Associated with Ivanti Connect Secure

Release Date: March 28, 2025

CISA has published a Malware Analysis Report (MAR) with analysis and associated detection signatures on a new malware variant CISA has identified as RESURGE. RESURGE contains capabilities of the SPAWNCHIMERA[1 <https://blogs.jpcert.or.jp/en/2025/02/spawnchimera.html>] malware variant, including surviving reboots; however, RESURGE contains distinctive commands that alter its behavior. These commands:

- Create a web shell, manipulate integrity checks, and modify files.
- Enable the use of web shells for credential harvesting, account creation, password resets, and escalating permissions.
- Copy the web shell to the Ivanti running boot disk and manipulate the running coreboot image.

RESURGE is associated with the exploitation of CVE-2025-0282 in Ivanti Connect Secure appliances. CVE-2025-0282 is a stack-based buffer overflow vulnerability in Ivanti Connect Secure, Policy Secure, and ZTA Gateways. CISA added CVE-2025-0282 to its Known Exploited Vulnerabilities Catalog <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> on January 8, 2025.

For more information on the abovementioned malware variants and YARA rules for detection, see: MAR-25993211.R1.V1.CLEAR. <https://www.cisa.gov/news-events/analysis-reports/ar25-087a>

For a downloadable copy of the SIGMA rule associated with this MAR, see: AR25-087A SIGMA YAML. </sites/default/files/2025-03/ar25-087a%20sigma%20yaml.pdf>

CISA urges users and administrators to implement the following actions in addition to the Mitigation Instructions for CVE-2025-0282 <https://www.cisa.gov/cisa-mitigation-instructions-cve-2025-0282>:

- **For the highest level of confidence, conduct a factory reset.**
  - **For Cloud and Virtual systems, conduct a factory reset using an external known clean image of the device.**
- See Ivanti's Recommended Recovery Steps for more information, including how to conduct a factory reset.
- Reset credentials of privileged and non-privileged accounts.

- Reset passwords for all domain users and all local accounts, such as Guest, HelpAssistant, DefaultAccount, System, Administrator, and krbtgt. The krbtgt account is responsible for handling Kerberos ticket requests as well as encrypting and signing them. The krbtgt account should be reset twice because the account has a two-password history. The first account reset for the krbtgt needs to be allowed to replicate prior to the second reset to avoid any issues. See CISA's Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise <https://www.cisa.gov/news-events/analysis-reports/ar21-134a> for more information. Although tailored to Federal Civilian Executive Branch (FCEB) agencies compromised in the 2020 SolarWinds Orion supply chain compromise, the steps are applicable to organizations with Windows AD compromise.

- Review access policies to temporarily revoke privileges/access for affected devices. If it is necessary to not alert the attacker (e.g., for intelligence purposes), then privileges can be reduced for affected accounts/devices to "contain" them.

- Reset the relevant account credentials or access keys if the investigation finds the threat actor's access is limited to non-elevated permissions.

- Monitor related accounts, especially administrative accounts, for any further signs of unauthorized access.

Organizations should report incidents and anomalous activity related to information found in the malware analysis report to CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. Malware submissions can be made directly to Malware Nextgen at https://malware.cisa.gov <https://malware.cisa.gov/>.

See the following resources for more guidance:

- Ivanti: Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-0282, CVE-2025-0283)

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we'd welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CISA Central

1-844-Say-CISA SayCISA@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>