# AL2026_02 CISA Warns That RESURGE Malware Can Remain Dormant on Ivanti Devices (March 2nd, 2026)

## Description

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a warning that a malware strain known as RESURGE can remain dormant on compromised Ivanti devices, even after patching and remediation efforts.

RESURGE is associated with exploitation of vulnerabilities in Ivanti Connect Secure (ICS) and related appliances. According to CISA, threat actors are deploying this malware to maintain persistent access, evade detection, and regain control of systems after organizations believe they have mitigated initial compromise.

This development poses significant risks to organizations using Ivanti remote access and VPN solutions, particularly within government, telecommunications, finance, and critical infrastructure sectors.

## Attack Details

RESURGE is a sophisticated malware variant deployed following exploitation of Ivanti Connect Secure vulnerabilities. It is designed to establish persistence and evade standard remediation procedures.

Key characteristics include:

- **Dormant persistence:** RESURGE can remain inactive for extended periods, avoiding detection by traditional monitoring tools and activating later to re-establish attacker control.
- **Post-patch survival:** Even after organizations apply security patches, the malware may persist if full remediation steps are not followed, giving attackers continued foothold within the environment.
- **Credential and configuration targeting:** Compromised devices may expose authentication data, configuration files, and session tokens, increasing the risk of lateral movement.
- **Stealth techniques:** The malware blends into legitimate processes and may leverage legitimate system functionality to reduce detection likelihood.

CISA has emphasized that simply applying patches is insufficient if devices were compromised prior to patching. In such cases, a factory reset and full rebuild may be required to ensure removal of persistent backdoors.

## Remediation

Given the risk of persistent compromise, organizations using Ivanti appliances should take the following actions immediately:

- **Follow CISA guidance:** Review and implement mitigation and recovery steps issued by the Cybersecurity and Infrastructure Security Agency (CISA), including integrity checks and forensic analysis of affected appliances.
- **Perform factory resets where necessary:** If compromise is suspected, conduct a full factory reset of Ivanti devices and rebuild using clean firmware images rather than relying solely on patching.
- **Apply latest patches:** Ensure all Ivanti Connect Secure, Policy Secure, and related products are updated to the most recent security releases.
- **Credential rotation:** Reset all administrative credentials, VPN user passwords, API keys, certificates, and authentication tokens associated with affected systems.
- **Hunt for indicators of compromise (IOCs):** Review logs for unusual administrative access, unauthorized file modifications, suspicious outbound connections, and abnormal authentication activity.
- **Network segmentation:** Isolate VPN and remote access infrastructure from core internal systems to limit lateral movement in case of compromise.
- **Enhanced monitoring:** Deploy continuous monitoring and EDR solutions capable of detecting anomalous behavior originating from network appliances.
- **Incident response activation:** If indicators of compromise are found, activate incident response procedures immediately, preserve logs, and notify relevant authorities as required.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

## References


- CISA warns that RESURGE malware can be dormant on Ivanti devices. (2026). Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/cisa-warns-that-resurge-malware-can-be-dormant-on-ivanti-devices/
- MAR-25993211-r1.v2 Ivanti Connect Secure (RESURGE). (2026). Retrieved from CISA. http://cisa.gov/news-events/analysis-reports/ar25-087a