MANDIANT
NOW PART OF Google Cloud

Remediation + Hardening Guide

Ivanti Connect Secure (CS)

CVE-2023-46805 / CVE-2024-21887 / CVE-2024-21888 / CVE-2024-21893 / CVE-2024-22024

v4.0

Summary

This document contains remediation and hardening recommendations for suspected compromised Ivanti Connect Secure (CS) VPN appliances associated with the exploitation of CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893, and CVE-2024-22024, announced by Ivanti on January 10, 2024, January 31, 2024, and February 8, 2024.

This guide provides containment, remediation, and hardening measures that should be considered to mitigate the impact of a compromised appliance.

Created: January 23, 2024
Updated: February 27, 2024

Change Log

Version	Date	Updates
1.0	Jan 23, 2024	Initial Document
2.0	Jan 31, 2024	Updated to include references to: • CVE-2024-21888 • CVE-2024-21893 • Official Patches
3.0	Feb 8, 2024	Updated to include references to: • CVE-2024-22024
4.0	Feb 27, 2024	Updated to include references to: • Persistence Across System Upgrades, Patches, and Factory Resets

Table of Contents

Background

On January 10, 2024, Ivanti disclosed two vulnerabilities, CVE-2023-46805 and CVE-2024-21887, impacting Ivanti Connect Secure (CS) VPN (fka Pulse Secure) and Ivanti Policy Secure (PS) appliances.

- CVE-2023-46805: Authentication Bypass (CVSS 8.2)
- CVE-2024-21887: Command Injection (CVSS 9.1)

On January 31, 2024, Ivanti disclosed two additional vulnerabilities, CVE-2024-21888 and CVE-2024-21893, impacting the same appliances and versions.

- CVE-2024-21888: Privilege Escalation (CVSS 8.8)
- CVE-2024-21893: Server-side forgery in the Security Assertion Markup Language (SAML) component (CVSS 8.2)

These vulnerabilities allow an unauthenticated actor to bypass authentication and execute arbitrary commands on a vulnerable appliance. Mandiant has identified zero-day exploitation of these vulnerabilities in the wild beginning as early as December 2023.

On January 31, 2024, Ivanti released the first round of patches to mitigate the identified vulnerabilities. Installation of the patch should be prioritized, as a mitigation bypass technique was recently identified that led to the deployment of a custom webshell. Ivanti is scheduled to continue rolling out additional patches over the coming weeks.

On February 8, 2024, Ivanti disclosed an additional vulnerability, CVE-2024-22024, impacting specific versions of appliances.

- CVE-2024-22024: XML eXternal Entity (XXE) vulnerability in the SAML component (CVSS 8.3)

With the identification of CVE-2024-22024, Ivanti released another patch to address the vulnerability for the specific versions of impacted appliances.
Per Ivanti, the patch released on February 8, 2024 *"replaces prior patches made available on 31 January and 1 February. We have no evidence of this vulnerability being exploited in the wild as it was found during our internal review and testing of our code."*
Organizations running appliances that are vulnerable to CVE-2024-22024 will **need to apply the latest patch released on February 8, 2024**. Ivanti also has noted that if a factory reset was completed prior to the installation of the patches released on January 31 or February 1, a *second* factory reset should not be required for installing the February 8 patch.

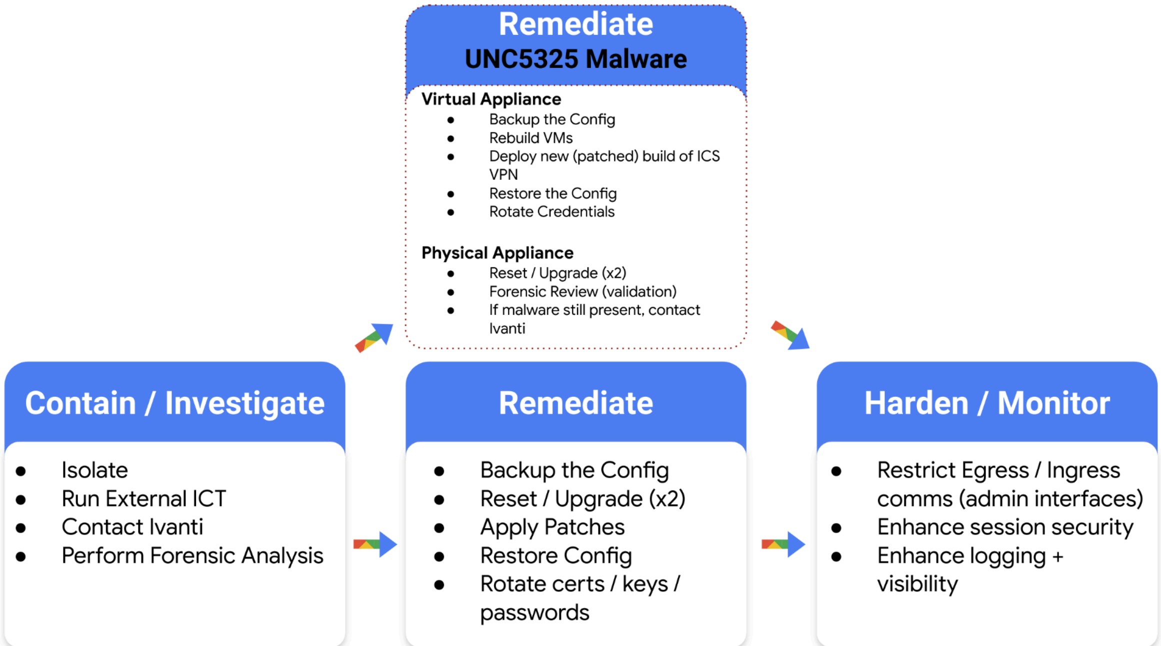
For appliances that do not yet have a patch available, Ivanti has provided a mitigation file (mitigation.release.20240126.5.xml) that must be applied to vulnerable appliances to address the five identified CVEs.

While installing the mitigation (XML file import) is intended to prevent future exploitation of the five vulnerabilities, it is not intended to remediate or otherwise contain an existing compromised device. Throughout numerous investigations, Mandiant has identified installation of backdoors on compromised appliances, in addition to other backdoors / web shells on other systems.

Disclosure Date	Ivanti ICS CVE	CVSS	Temporary Mitigation* mitigation.release.20240126.5.xml	Staged Patches 01/31/24 Initial Release Date	Staged Patches 02/08/24 Initial Release Date
01/10/24	CVE-2023-46805	8.2	✓	✓	✓
01/10/24	CVE-2024-21887	9.1	✓	✓	✓
01/31/24	CVE-2024-21888	8.8	✓	✓	✓
01/31/24	CVE-2024-21893	8.2	✓	✓	✓
02/08/24	CVE-2024-22024	8.3	✓	✗	✓

* The temporary mitigation will block all SAML communication and authentication. Per Ivanti, "As a workaround, customers who use SAML for authentication can establish LDAP authentication for administrators and high priority users while the staggered patches are in development."

On February 27, 2024 Mandiant released details on UNC5325 attempting to persist across factory resets, system upgrades, and patches. For these specific instances, Mandiant has updated our remediation guidance within this document.


Remediate
UNC5325 Malware
Virtual Appliance
Backup the Config
Rebuild VMs
Deploy new (patched) build of ICS VPN
Restore the Config
Rotate Credentials
Physical Appliance
Reset / Upgrade (x2)
Forensic Review (validation)
If malware still present, contact Ivanti
Contain / Investigate
Isolate
Run External ICT
Contact Ivanti
Perform Forensic Analysis
Remediate
Backup the Config
Reset / Upgrade (x2)
Apply Patches
Restore Config
Rotate certs / keys / passwords
Harden / Monitor
Restrict Egress / Ingress comms (admin interfaces)
Enhance session security
Enhance logging + visibility

Containment and Investigative Preparation Steps

Mandiant recommends that organizations that are running impacted version(s) of the appliance(s) follow the processes outlined below for immediate containment and investigative actions.

- Isolate the impacted appliance(s).
- Run the external integrity checker tool (ICT) to identify potential signs of compromise. Ivanti recommends running the *external* ICT, as it is updated more frequently and is more resistant to malicious tampering.

Note: The ICT does not scan for malware or other Indicators of Compromise (IOCs). The scan results alone should not be the sole basis for determining if an appliance is compromised.

- Provide Ivanti support with the output from the ICT to review the results.
  - Ivanti can also provide assistance with decryption and capturing a forensic / memory image from the impacted appliance(s).
- Perform a forensic review of the captured image(s) to identify additional signs of compromise or malicious activities.
- Review available logs from the appliance(s), including:
  - VPN device logs - accessed via *System > Log/Monitoring* from the administrative interface. The logs can then be viewed on the web or exported for offline analysis.
  - Unauthenticated Request logging - which can be configured via:

```
System > Log/Monitoring > User Access > Select Events to Log
```

With this setting configured, unauthenticated web requests made to the CS VPN appliance(s) are recorded in the user logs. This can potentially help with identifying exploitation, data exfiltration, or other events related to an attacker attempting to gain unauthorized access to the device.

  - Syslog forwarding can also be configured to ensure that appliance logs are available offline from the appliance and cannot be modified. At a minimum, Mandiant recommends that the following log types be configured for syslog forwarding:
    - Events
    - User Access
    - Admin Access

For additional details related to post exploitation findings and analysis, reference:

- Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation
- Cutting Edge Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation
- Cutting Edge, Part 3: Investigating Ivanti Connect Secure VPN Exploitation and Persistence Attempts

Remediation Steps

Per Ivanti, *"if exploitation has occurred, we believe it is likely that the threat actor has taken an export of your running configurations with the private certs loaded on the gateway at time of exploit and left behind a Web shell file enabling backdoor future access."*

Before returning an impacted appliance back into production, the following processes should be followed.

- **Preserve a forensic image from the impacted appliance(s)** for forensic analysis and investigative purposes.
- **If any evidence of UNC5325 malware is identified as published in Cutting Edge, Part 3, Mandiant recommends the following:**
    - For virtual appliances:
        - Backup existing configurations
        - Rebuild impacted virtual machines
        - Deploy a new build of Ivanti Connect Secure VPN
        - Restore configuration(s) from backup
        - Revoke or rotate any device credentials (detailed below)
    - For physical appliances:
        - Perform the Factory Reset as detailed below followed by a forensic image to confirm no malware persistence. If additional validation is required, contact Ivanti for further guidance.

For investigations that **did not** yield evidence of UNC5325 malware:

- **Backup the configuration of the appliance.**
- **Factory reset or upgrade the appliance TWICE.**
    - When upgrading, any exploited or added files on the device will not persist through the upgrade.
    - Future rollbacks would make an organization vulnerable if restoring to the compromised version. **Two upgrades removes the compromised version - as only one rollback version is stored on the appliance.**
- **Download and apply the official patch (February 8, 2024)** that remediates CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893, and CVE-2024-22024.
  Note: If a previous mitigation (XML file) was applied before the patch, it can be removed once the patch has been applied. The mitigation removal XML process can be found in the download portal.
- **If a formalized patch is not yet available** for a vulnerable appliance:

    - **Apply the mitigation patch** (via importing the mitigation.release.20240126.5.xml file) after the upgrade has been completed.
        - Note: Applying the XML file may impact functionality and features of an appliance, including SAML authentication.
    - **Stop the push of configurations to appliances** once the XML file is in place, and do not resume pushing configurations until formal patches have been issued by Ivanti. This includes any configurations that are pushed using Pulse One and/or nSA. **Pushing configurations to an appliance will stop the short-term mitigation from functioning.**
- **Restore the device configuration.**
- **Revoke or rotate any device specific secrets stored on the appliance prior to compromise.**
    - **Revoke and reissue any stored certificates** that were present on impacted appliance(s).
        - Certificates used for device and/or user authentication (such as client certificates and server certificates) would be included in this, along with code signing certificates and the SSL certificate on the external interface(s).
    - **Reset the *admin enable* password**.
    - **Reset any API keys** stored on the appliance(s).
    - **Reset the password of any local user(s) defined on the appliance(s).**
        - This could include service accounts used for third-party integrated authentication configurations.
- **If any credential stealers are identified on an appliance, reset the passwords** for any users that authenticated to the appliance during the period when the malware was active. This may require that organizations consider an enterprise password reset as part of a full remediation strategy.

Additional Hardening Measures

Based on the scope of the investigation, additional [hardening measures] *may* be required. Many of these recommendations align to best practices, and may not be prescriptive for mitigating the impact of each compromise.

- **Restrict egress communications from the CS VPN appliance(s).** This can mitigate the impact of command-and-control (C2) communications from any backdoors that are present on an appliance.

- **Disable administrative access to the CS VPN appliance(s) from the external (internet-facing) port.**

```
Administrator > Admin Realms > Select Realm > Authentication Policy >
Source IP > Ensure that “Enable administrators to sign in on the External
Port” is not enabled.
```

- **Minimize the scope of internal connectivity paths that could be leveraged for lateral movement from the management interface of CS VPN appliance(s).**
  - If the appliance(s) are configured with a one-arm topology, the following hardening measures should be considered:
    - Enable **Source IP Based Restrictions** for the Administrator Realm.

```
Administrators > Admin Realms > Admin Users > Authentication Policy >
Source IP
```

    - Enable **MFA** for the administrator sign-in URL.
    - Configure the **Management Port** to allow administrators to sign in and disable administrators to sign in on the Internal Port.

```
Administrators > Admin Realms > Admin Users > Authentication Policy >
Administrator sign in ports
```

- **Disable Session Roaming** - which can mitigate the impact of a stolen session cookie being reused by a different IP address that does not correlate to the initial user who logged in.

```
Users: Users > User Roles > <role name> > General > Session Options:
Roaming Session, select "Disabled"
```

Admins: Administrators > Admin Roles > <role name> > General > Session Options: Roaming Session, select "Disabled"

- **Enforce Session Lifetime Limits** to reduce the risk of a stolen session being continuously reused by an attacker. Mandiant recommends session lengths of 8-12 hours, although this may need to be adjusted based upon business needs and requirements.

Users: Users > User Roles > <role name> > General > Session Options: Session lifetime lengths

Admins: Administrators > Admin Roles > <role name> > General > Session Options: Session lifetime lengths

- **Do not allow Persistent Sessions** to reduce the risk of a stolen session being continuously reused by an attacker.

Users: Users > User Roles > <role name> > General > Session Options: Persistent Session, select "Disabled"

Admins: Administrators > Admin Roles > <role name> > General > Session Options: Persistent Session, select "Disabled"

- **Enable "Remove Browser Session Cookies"** to reduce the risk of stealing browser session cookies.

Users: Users > User Roles > <role name> > General > Session Options: Remove Browser Session Cookie, select "Enabled"

Admins: Administrators > Admin Roles > <role name> > General > Session Options: Remove Browser Session Cookie, select "Enabled"

- **Enable "HTTP Only Device Cookie"** to reduce the risk of cookie stealing.

Users: Users > User Roles > <role name> > General > Session Options: HTTP Only Device Cookie, select "Enabled"

Admins: Administrators > Admin Roles > <role name> > General > Session Options: HTTP Only Device Cookie, select "Enabled"