Security Advisory 2024-004

Critical Vulnerabilities in Ivanti Connect Secure

February 9, 2024 — v1.5

TLP:CLEAR

History:

- *11/01/2024 — v1.0 – Initial publication*
- *16/01/2024 — v1.1 – Adding patch schedule and information about remediation*
- *23/01/2024 — v1.2 – Adding information about race condition when pushing configurations*
- *31/01/2024 — v1.3 – Adding information about new vulnerabilities*
- *07/02/2024 — v1.4 – Update the recommendations section*
- *09/02/2024 — v1.5 – Adding information about new vulnerability*

Summary

On January 10, 2024, Ivanti has released an advisory about two critical vulnerabilities [1,2] in Ivanti Connect Secure (ICS) and Policy Secure gateways. These vulnerabilities, identified as **CVE-2023-46805** and **CVE-2024-21887**, have been exploited in the wild and can allow remote attackers to execute arbitrary commands on targeted gateways.

On January 31, 2024, Ivanti has released an advisory about two new critical vulnerabilities [2] in Ivanti Connect Secure (ICS) and Policy Secure gateways. These vulnerabilities are identified as **CVE-2024-21888** and **CVE-2024-21893**. **CVE-2024-21893** have been exploited in the wild chained with **CVE-2024-21887** and can lead to remote attackers to execute arbitrary commands on targeted gateways.

[New] On February 8, 2024, Ivanti has released an advisory about a new critical vulnerability in Ivanti Connect Secure (ICS) and Policy Secure gateways. The vulnerability tracked as **CVE-2024-22024** is a new authentication bypass [6]. While Ivanti claims that this vulnerability was found during their internal review and testing of their code, Watchtowr researchers claim otherwise [7].

Technical Details

The first vulnerability, **CVE-2023-46805** with a CVSS score of 8.2, is an authentication bypass in the gateways web component. This flaw enables attackers to access restricted resources by circumventing control checks.

The second vulnerability, **CVE-2024-21887** with a CVSS score of 9.1, is a command injection vulnerability that allows authenticated administrators to execute arbitrary commands on vulnerable appliances by sending specially crafted requests.

The third vulnerability, **CVE-2024-21888** with a CVSS score of 8.8, is a privilege escalation vulnerability in the web component that can allow a user to elevate privileges to that of an administrator.

The fourth vulnerability, **CVE-2024-21893** with a CVSS score of 8.2, is a server-side request forgery vulnerability in the SAML component that can allow an attacker to access certain restricted resources without authentication.

[New] The fifth vulnerability, **CVE-2024-22024** with a CVSS score of 8.3 , is an authentication bypass vulnerability involving an XML external entity or XXE vulnerability in the SAML component.

When those vulnerabilities are combined, attackers can run arbitrary commands on all supported versions of the impacted products without requiring authentication.

Affected Products

All supported versions of Ivanti Connect Secure (ICS) and Policy Secure gateways.

Ivanti released the patch availability schedule by version [2].

Version	Product	Target Week
9.1R14x	Ivanti Connect Secure	Week of 29 January
9.1R15x	Ivanti Connect Secure	Week of 12 February
9.1R16x	Ivanti Connect Secure	Week of 29 January
9.1R17x	Ivanti Connect Secure	Week of 22 January
9.1R18x	Ivanti Connect Secure	Week of 22 January
22.1R6x	Ivanti Connect Secure	Week of 19 February
22.2R4x	Ivanti Connect Secure	Week of 12 February
22.3R1x	Ivanti Connect Secure	Week of 29 January
22.4R1x	Ivanti Connect Secure	Week of 12 February
22.4R2x	Ivanti Connect Secure	Week of 22 January
22.5R1x	Ivanti Connect Secure	Week of 22 January
22.5R2x	Ivanti Connect Secure	Week of 19 February
22.6R1x	Ivanti Connect Secure	Week of 12 February
22.6R2x	Ivanti Connect Secure	Week of January 29
22.5R1x	ZTA	Week of 29 January
22.6R1x	ZTA	Week of 22 January

[New] The vulnerability affects a limited number of versions for which a patch is available already:

- Ivanti Connect Secure versions 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1;
- Ivanti Policy Secure version 22.5R1.1;
- ZTA version 22.6R1.3.

Recommendations

All the supported products are vulnerable. Ivanti has provided early-access patches, for the various product versions as follows:

Product	Product version	Patch availability
Ivanti Connect Secure	9.1R18.3	ICS_9.1_R18.3_package-24995.1.pkg
Ivanti Connect Secure	22.4R2.2	ICS_22.4R2.2_package-2149.1.pkg
Ivanti Connect Secure	22.5R1.1	ICS_22.5R1.1_package-2175.1.pkg
Ivanti Connect Secure	9.1R14.4	Contact Ivanti Support
Ivanti Connect Secure	9.1R17.2	Contact Ivanti Support
Ivanti ZTA	22.6R1.3	Contact Ivanti Support

CERT-EU recommends proceeding as follows:

- Immediate actions:
  - apply mitigation;
  - acquire forensic evidence (disk image and memory) to perform a compromise assessment;
  - apply the remediation steps.
- If the above cannot be implemented:
  - take the affected Ivanti products offline until you can;

When it is not possible or too late to perform the compromise assessment, it is recommended applying the "assume compromise" scenario [5]. It is then advised to: - reset local users' password (including the one of the service accounts used for auth server configuration); - revoke and replace any private certificate that was installed on the ICS; - hunt for suspicious events during the past weeks (suspicious authentication, recently created privileged users, etc.)

[New] As for the vulnerability **CVE-2024-22024**:

- If the process desbribed above (i.e., see immediate actions) has been performed, CERT-EU recommends applying the patches available as soon as possible [6].
- If the process desbribed above (i.e., see immediate actions) has not been performed, CERT-EU recommends applying the update as par of the remediation actions.

Mitigation

[Updated] The zero-days can be mitigated by importing the `importing mitigation.release.20240126.5.xml` file available to customers via Ivanti's download portal [2]. As the vulnerabilities affect critical functionality of the affected Ivanti systems, applying the mitigation file (rather than patching) can have serious adverse effects on their operation. This mitigation successfully blocks the vulnerability **CVE-2024-22024**.

As per Ivanti, customers should stop pushing configurations to appliances having the mitigation in place until the appliance is patched [2]. If configurations are pushed while the mitigation is in place, it will stop the mitigation from functioning and leave the appliances vulnerable.

As per Ivanti, the provided mitigation blocks the exploitation of vulnerabilities and prevents further use of the webshell.

Compromise assessment

Ivanti advises customers to run the external Integrity Checker Tool (ICT) [3]. However, the ICT will scan a snapshot of the current state of the appliance and cannot necessarily detect threat

actor activity if they have returned the appliance to an apparent clean state.

To assess with certainty if a device has (or had) been compromised, a forensic image of the device should be performed by contacting Ivanti support. As the external ICT will reboot the system, it is advised to take forensic evidence before running it.

Remediation

It is recommended factory resetting and upgrading, or upgrading twice the affected Ivanti systems. Ivanti shared the recovery steps related to those vulnerabilities [4].

[Updated] Note: Ivanti does not recommend resetting the appliances for customers who applied the patch released on January 31 or 1 February and completed a factory reset [6].

References

[1] https://www.bleepingcomputer.com/news/security/ivanti-warns-of-connect-secure-zero-days-exploited-in-attacks/

[2] https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

[3] https://forums.ivanti.com/s/article/KB44755?language=en_US

[4] https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US

[5] https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure

[6] https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

[7] https://labs.watchtowr.com/are-we-now-part-of-ivanti/