aDvens

Security for the greater good

Newscast
Vulnerability in Ivanti

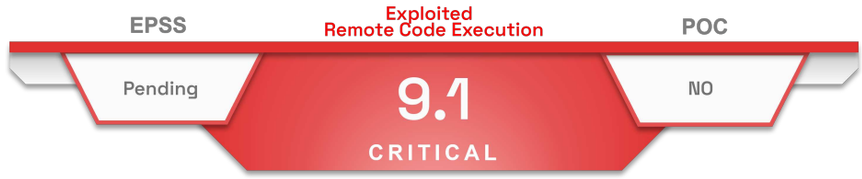
2024-01-11 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

IVANTI

Ivanti published a security advisory on 10 January 2024 concerning two vulnerabilities in *Ivanti Connect Secure* (ICS) and *Ivanti Policy Secure gateways*.

CVE-2024-21887



A command injection vulnerability in the web components of *Ivanti Connect Secure* and *Ivanti Policy Secure* has been discovered by Volexity security researchers.

By sending a specifically crafted request, a remote and authenticated attacker can execute arbitrary code.

The CVE-2024-21887 (arbitrary code execution) can be exploited in conjunction with CVE-2023-46805 (authentication bypass).

Volexity observed the exploitation of this vulnerability and attributed it to the UTA0178 group.
CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on January 10, 2024.

Type of vulnerability

- **CWE-77**: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Risks

- Remote Code Execution

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	High	Impact on integrity	High
User Interaction	None	Impact on availability	High

Proof of concept

To date, no proof of concept is available in open source.

CVE-2023-46805

An authentication check flaw in the web components of *Ivanti Connect Secure* and *Ivanti Policy Secure* has been discovered by Volexity security researchers.

Exploitation of this vulnerability by a remote, unauthenticated attacker can bypass security controls and gain access to web service information.

Volexity observed the exploitation of this vulnerability and attributed it to the UTA0178 group.
CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on January 10, 2024.

Type of vulnerability

- **CWE-287** : Improper Authentication

Risks

- Bypass security policy

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	Low
User Interaction	None	Impact on availability	None

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Proof of concept

To date, no proof of concept is available in open source.

Affected products

- Ivanti Connect Secure Ivanti Policy Secure gateways versions 9.x to 22.x

Recommendations

- There is as yet no patch proposed by the editor. A first corrected version should be made available during the week of January 22, with the final version due for release during the week of February 19.
- Ivanti offers a workaround by importing the *mitigation.release.20240107.1.xml* file via their download portal. The procedure for installing this workaround is available on their KB article.
- Additional information is available in Ivanti's advisory.

Sources

Ivanti

- https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
- 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?language=en_US
- https://www.cisa.gov/news-events/alerts/2024/01/10/ivanti-releases-security-update-connect-secure-and-policy-secure-gateways
- https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

CVE-2024-21887

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-21887

CVE-2023-46805

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46805