



Ivanti Connect Secure and Policy Secure Attack

Zero-day vulnerabilities actively exploited

<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>
 CVEs: CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893, CVE-2024-22024

Widespread exploitation of zero-day vulnerabilities affecting Ivanti Connect Secure and Policy Secure gateways underway.

Background CVE-2023-46805 is an Authentication Bypass Vulnerability found in the web component of Ivanti Connect Secure (ICS) and Ivanti Policy Secure to allow a remote attacker to access restricted resources by bypassing control checks. CVE-2024-21887 is a command injection vulnerability in web components of ICS and Ivanti Policy Secure. If CVE-2024-21887 is used in conjunction with CVE-2023-46805, exploitation does not require authentication and enables a threat actor to craft malicious requests and execute arbitrary commands on the system.

Announced Jan 10, 2024: Ivanti disclosed two new vulnerabilities in their ICS and Ivanti Policy Secure gateways: CVE-2023-46805 and CVE-2024-21887.
<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>

Latest Developments Jan 18, 2024: FortiGuard Labs released a Threat Signal on Ivanti Connect Secure and Policy Secure Gateways Zero-day Vulnerabilities (CVE-2023-46805 and CVE-2024-21887)
<https://www.fortiguard.com/threat-signal-report/5371/>

Jan 19, 2024: CISA Issues Emergency Directive to Federal Agencies on Ivanti Zero-Day Exploits. This Directive requires agencies to implement Ivanti's published mitigation immediately to the affected products in order to prevent future exploitation
<https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities>

Jan 22, 2024: FortiGuard Labs has released IPS signatures to detect and block Authentication Bypass (CVE-2023-46805) and Server-Side Request Forgery Vulnerability (CVE-2024-21893) is observing high IPS activity since the release of the signatures.

Jan 22, 2024: Ivanti plans to begin releasing patches addressing these vulnerabilities on a schedule. Until patches are available, Ivanti has provided a workaround for the users to mitigate exploitation risks
<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>

Feb 01, 2024: Ivanti identified additional vulnerabilities in ICS and Ivanti Policy Secure, and Ivanti Neurons for ZTA. CVE-2024-21888 allows for privilege escalation and CVE-2024-21893 is a server-side request forgery in the SAML component which allows a threat actor to access certain restricted resources without authentication. Vendor mentions in the advisory that CVE-2024-21893 appears to be seen in some targeted attacks and expects an increase in the attacks. CVE-2024-21893 has also been added to CISA's known exploited vulnerability catalog (KEV).

Feb 9, 2024: Ivanti disclosed a fifth vulnerability- CVE-2024-22024 (XXE) for ICS and Ivanti Policy Secure.
https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

Feb 13, 2024: A new report by Orange Cyberdefense shows attackers using CVE-2024-21893 to install a new backdoor named DSLog.
https://www.orange cyberdefense.com/fileadmin/general/pdf/Ivanti_Connect_Secure_-_Journey_to_the_core_of_the_DSLog_backdoor.pdf

Please note, this is an ongoing investigation and as the situation is evolving, FortiGuard Labs will update and add new protections accordingly.

Feb 29, 2024: CISA released a Cybersecurity Advisory on Threat Actors Exploiting Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways
<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure

Redirect an attacker to engage with a decoy instead of a real Ivanti Connect Secure and Policy Secure Devices

FortiDeceptor
DB 20240227

Decoy VM

Detects attack attempts and monitor malicious activities on the network

FortiDeceptor
DB 20240227

Weaponization

Delivery

AV

Detect and block attack known malware related to Ivanti Connect Secure and Policy Secure Attack

FortiGate
DB 92.0119

FortiWeb
DB 92.0119

FortiClient
DB 92.0119

FortiSASE
DB 92.0119

FortiCASB
DB 92.0119

FortiCWP
DB 92.0119

FortiADC
DB 92.0119

FortiProxy
DB 92.0119

AV (Pre-filter)

Detect and block attack known malware related to Ivanti Connect Secure and Policy Secure Attack

FortiEDR
DB 92.0119

FortiNDR
DB 92.0119

Exploitation

IPS

Detect and block attack attempts targeting Ivanti Connect Secure and Policy Secure

FortiGate
DB 26.718

FortiSASE
DB 26.718

FortiNDR
DB 26.718

FortiADC
DB 26.718

FortiProxy
DB 26.718

Web App Security

Detect and block attack attempts targeting Ivanti Connect Secure and Policy Secure Authentication Bypass

FortiWeb
DB 0.00368

Installation

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

FortiAnalyzer

FortiSIEM

FortiSOCaaS

Outbreak Detection

FortiAnalyzer
DB 2.00036

FortiSIEM
DB 604

FortiNDR Cloud
v2024.3+

Threat Hunting

FortiAnalyzer
v6.4+

FortiNDR Cloud
v2024.3+

Playbook

FortiSOAR
v7.4.0+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training

Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

- Ivanti** https://forums.ivanti.com/s/article/Recovery-Steps-Related-to-CVE-2023-46805-and-CVE-2024-21887?language=en_US
- HelpNet Security** <https://www.helpnetsecurity.com/2024/01/11/cve-2023-46805-cve-2024-21887/>
- The Hacker News** <https://thehackernews.com/2024/01/cisa-issues-emergency-directive-to-hml>
- Ivanti's integrity checker** https://forums.ivanti.com/s/article/KB44755?language=en_US
- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/hackers-exploit-ivanti-ssrf-flaw-to-deploy-new-dslog-backdoor/>

Learn more about [FortiGuard Outbreak Alerts](#)