National Cyber Security Centre

2401100123-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Vulnerabilities Discovered Within Ivanti Products

Update 1.2

Thursday 1st February, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	10th January 2024	CSIRT-IE	Initial advisory
1.1	11th January 2024	CSIRT-IE	Update with details of exploitation and IOCs
1.2	1st February 2024	CSIRT-IE	Update with details of new CVEs

Description

Vulnerabilities have been discovered in Ivanti Connect Secure (ICS), (formerly known as Pulse Connect Secure) and Ivanti Policy Secure gateways which affect all supported versions.

CVE-2023-46805 is a bypass vulnerability in the web component of Ivanti Connect Secure and Ivanti Policy Secure with CVSS 8.2. This vulnerability allows a remote attacker to access restricted resources by bypassing control checks.

CVE-2024-21887 is a command injection vulnerability in the web component of Ivanti Connect Secure and Ivanti Policy Secure with CVSS 9.1. This vulnerability allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. This vulnerability can be exploited over the internet.

The Ivanti Neurons for ZTA gateways cannot be exploited when in production. If a gateway for this solution is generated and left unconnected to a ZTA controller, then there is a risk of exploitation on the generated gateway. Ivanti Neurons for Secure Access is not vulnerable to these CVEs, however the gateways being managed are independently vulnerable to these CVEs. For this reason, Ivanti Neurons for ZTA is included in the patch.

You can view the Ivanti advisory here: https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways.

Update 1.2:
On January 31, 2024, Ivanti updated their security advisory to indicate the release of patches for the authentication bypass (**CVE-2023-46805**) and command injection (**CVE-2024-21887**) vulnerabilities impacting Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) gateways.

Ivanti also disclosed two additional vulnerabilities affecting their Connect Secure, Policy Secure, and Neurons for ZTA products:

- **CVE-2024-21888**: A privilege escalation vulnerability in web component allows a user to elevate privileges to that of an administrator.
- **CVE-2024-21893**: A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

Please review the Ivanti alert for further information

On January 31, 2024, Mandiant published a blog detailing additional tactics, techniques, and procedures (TTPs) detailing post-exploitation activity and have published indicators of compromise and signatures to aid in the detection of compromise. https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation

Products Affected

These vulnerabilities impact all supported versions of Ivanti Connect Secure Version 9.x and 22.x and Ivanti Policy Secure gateways.

Impact

Exploitation of CVE-2023-46805 could allow a remote attacker to access restricted resources by bypassing control checks.

Exploitation of CVE-2024-21887 could allow an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. This vulnerability can be exploited over the internet.

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.

The NCSC is aware of exploitation of these vulnerabilities. Further exploitation details can be found at the following link: https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

Recommendations

Ivanti recommends administrators perform the following tasks to identify if their appliances have been compromised.

1. A patch is now available via the standard download portal for Ivanti Connect Secure (versions 9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2 and 22.5R1.1), and ZTA version 22.6R1.3.
    - CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, and CVE-2024-21893 are all remediated with the patch.
2. There is a new mitigation available to address additionally identified vulnerabilities while the rest of the patches are in development to prioritise the best interest of our customers. If customers have applied the patch, they do not need to apply the mitigation. Customers can review the mitigation steps here.
3. Review the Internal Integrity Check Tool (ICT) logs. The following entries can be used to check the internal ICT logs:
    - SYS32039 - New files were found with the Internal Integrity Check Tool.
    - SYS32040 - A modified file was found with the Internal Integrity Check Tool.

- SYS32041 - The Integrity Check Tool manifest file is missing.
- SYS32042 - The Integrity Checker Tool manifest file is bad.
- SYS32087 - A built-in integrity scan has started.
- SYS32088 - A built-in integrity scan has been completed.

4. If there is **no signs of compromise** within the Internal ICT logs, Ivanti are advising that customers run the External Integrity Check Tool (ICT). The External ICT should only be ran if the Internal ICT **does not indicate** signs of compromise. This is to preserve the memory as the External ICT requires a system reboot.
    - The External ICT can be downloaded from here.
5. Review the following logs to ensure the External ICT has been ran successfully.
    - SYS32101 - An External Integrity Checker Tool scan has started.
    - SYS32102 - An External Integrity Checker Tool scan has been completed.
6. Perform a network scan of the appliance to ensure no unusual ports or services are running.
7. Review outbound network traffic from the device. The table below contains IOCs reported by Volexity which have bee observed during the compromise of the Ivanti devices.

Indicators Of Compromise

IOC	Description
gpoaccess[.]com	Suspected domain. Discovered via domain registration patterns.
webb-institute[.]com	Suspected domain. Discovered via domain registration patterns.
symantke[.]com	Domain used to collect credentials from compromised devices.
206[.]189[.]208[.]156	DigitalOcean IP address tied to threat actor.
75[.]145[.]243[.]85	IP address observed interacting with compromised device.
47[.]207[.]9[.]89	IP address observed interacting with compromised device.
98[.]160[.]48[.]170	IP address observed interacting with compromised device.
173[.]220[.]106[.]166	IP address observed interacting with compromised device.
73[.]128[.]178[.]221	IP address observed interacting with compromised device.
50[.]243[.]177[.]161	IP address observed interacting with compromised device.

50[.]213[.]208[.]89	IP address observed interacting with compromised device.
64[.]24[.]179[.]210	IP address observed interacting with compromised device.
75[.]145[.]224[.]109	IP address observed interacting with compromised device.
50[.]215[.]39[.]49	IP address observed interacting with compromised device.
71[.]127[.]149[.]194	IP address observed interacting with compromised device.
173[.]53[.]43[.]7	IP address observed interacting with compromised device.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie