National Cyber Security Centre

2402090128-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

XXE Vulnerability affecting Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways CVE-2024-22024 - CVSS 8.3

Friday 9th 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.

Description

An XML external entity or XXE vulnerability has been discovered affecting the Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways - **(CVE-2024-22024)**.

Further information can be found here: https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US.

This vulnerability is due to an XXE (XML eXternal Entities) weakness in the gateways' SAML component that allows remote attackers gain access to restricted resources on unpatched appliances in low-complexity attacks **without requiring** user interaction or authentication.

This vulnerability is in addition to recently disclosed vulnerabilities affecting Ivanti products. Further details related to those vulnerabilities can be found here: https://www.ncsc.gov.ie/pdfs/01_02_24_Ivanti_Advisory.pdf

CVE-2024-22024 is an XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x), Ivanti Policy Secure (9.x, 22.x) and ZTA gateways which allows an attacker to access certain restricted resources without authentication.

Products Affected

The vulnerability affects a limited number of supported versions:

- Ivanti Connect Secure (version 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

Impact

Exploitation would allow an attacker to access certain restricted resources without authentication. Ivanti have stated that they have currently no evidence of this vulnerability being exploited in the wild as it was found during internal review and testing.

Recommendations

It is **critically important** that affected organisations take urgent action in order to ensure that devices are fully protected using the patch released on 8 February 2024.

Customers who applied the patch released on 31 January or 1 February, and completed a factory reset of their appliance **need to apply this latest patch** and not factory reset their appliances again.

Ivanti also recommend that customers run Ivanti's previously released External Integrity Checker Tool and apply Ivanti's guidance on best practice, which includes advice that all customers perform a factory reset of their appliance before applying the patch, in order to prevent the threat actor from gaining persistence in your environment. If a customer completed a factory reset of their appliance before applying the previously released patches, **there is no need to perform a factory reset again**:

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

https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways-282024

It is highly recommended that Ivanti customers also reference the Volexity blog post and the Mandiant blog post which contain additional information on investigating and responding to potential compromise of Ivanti devices.

Recent Ivanti Vulnerabilities

Overview of Recent vulnerabilities affecting Ivanti Products:

CVE	Description	CVSS
CVE-2023-46805	An authentication bypass vulnerability in the web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.	8.2
CVE-2024-21887	A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance. This vulnerability can be exploited over the internet.	9.1
CVE-2024-21888	A privilege escalation vulnerability in web component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows a user to elevate privileges to that of an administrator.	8.8
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.	8.2
CVE-2024-22024	An XML external entity or XXE vulnerability in the SAML component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) which allows an attacker to access certain restricted resources without authentication.	8.3

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