Threat Intelligence Report: CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 ve CVE-2024-21893

This report examines attack models, potential impacts and associated IOCs related to vulnerabilities CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 and CVE-2024-21893.

CISA added 4 Ivanti-related vulnerabilities to its Catalog of Known Exploited Vulnerabilities in January.

CVE-2023-46805 and CVE-2024-21887 were added on January 10, and CVE-2024-21893 and CVE-2024-21888 were added on January 31.

CVE	Description	CVSSv3	Advisory
CVE-2023-46805	Ivanti Connect Secure and Ivanti Policy Secure Authentication Bypass Vulnerability	8.2	Released January 10
CVE-2024-21887	Ivanti Connect Secure and Ivanti Policy Secure Command Injection Vulnerability	9.1	Released January 10
CVE-2024-21888	Ivanti Connect Secure and Ivanti Policy Secure Privilege Escalation Vulnerability	8.8	Released January 31
CVE-2024-21893	Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability	8.2	Released January 31

CVE-2023-46805 ve CVE-2024-21887

CVE-2023-46805: This vulnerability allows attackers to bypass authentication on the web server, granting unauthorized access to internal resources.

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N ⇒ **Base Score:** 8.2 HIGH
- **Description:** Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability
- **Affected Versions:**
  - Ivanti Connect Secure versions 9.x and 22.x
  - Ivanti Policy Secure versions 9.x Ivanti
  - Policy Secure versions 22.x

CVE-2024-21887: This vulnerability allows an authenticated attacker to inject arbitrary commands into the system, potentially leading to complete system takeover.

- CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H ⇒ **Base Score:** 9.1 CRITICAL
- **Description:** Ivanti Connect Secure and Policy Secure Command Injection Vulnerability
- **Affected Versions:**
  - Ivanti Connect Secure versions 9.x and 22.x
  - Ivanti Policy Secure versions 9.x Ivanti
  - Policy Secure versions 22.x

Attack Models and Potential Impact

This joint analysis report examines two hypothetical vulnerabilities, namely CVE-2023-46805 and CVE-2024-21887, focusing on their respective attack models, potential impacts, and Indicators of Compromise (IOCs). It is essential to emphasize that both CVEs mentioned herein do not exist at the time of writing. However, the purpose remains to provide insight into handling discovered vulnerabilities in general.

CVE-2023-46805 Details:

- **Attack Model:**
  - Assuming CVE-2023-46805 enables remote code execution (RCE), attackers can send crafted HTTP requests to trigger the flaw without proper authentication checks.
- **Potential Impact:**
  - Successful exploitation may grant unauthorized access, allowing adversaries to steal sensitive data, disrupt services, or further escalate privileges within the targeted system.

CVE-2024-21887 Details:

- **Attack Model:**
  - Presume CVE-2024-21887 facilitates privilege escalation through local exploitation. A prerequisite assumes an authenticated session under limited permissions.
- **Potential Impact:**
  - By successfully exploiting this vulnerability, an attacker can obtain higher-level access than initially granted, enabling them to manipulate sensitive configurations or access restricted data stores.

Indicators of Compromise (IOCs)

The IOCs included in the "Vulnerability in Ivanti" report published by aDvens on January 31, 2024 are as follows.

IP Addresses:

- 206.189.208[.]156
- 75.145.243[.]85
- 47.207.9[.]89
- 98.160.48[.]170
- 173.220.106[.]166
- 73.128.178[.]221
- 50.243.177[.]161
- 50.213.208[.]89
- 64.24.179[.]210
- 75.145.224[.]109
- 50.215.39[.]49
- 71.127.149[.]194
- 173.53.43[.]7

Domains:

- gpoaccess[.]com
- webb-institute[.]com

Filenames:

- compcheckresult.cgi
- sessionserver.sh
- lastauthserverused.js
- visits.py
- sessionserver.pl
- libsecure.so.1
- cav-0.1-py3.6.egg

Conclusion and Recommendation

On January 10, Ivanti does not have patches to address these vulnerabilities. However, they have released a mitigation file (mitigation.release.20240107.1.xml) that can be used immediately until patches are released.

Update: Ivanti released their new patch on January 31st.

CVE-2024-21888 ve CVE-2024-21893

CVE-2024-21888: Ivanti Connect Secure and Ivanti Policy Secure's web component has a Privilege Escalation vulnerability. This vulnerability allows a user to gain administrative privileges. This is due to inadequate security restrictions in the web interface.

- CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H ⇒ **Base Score:** 8.8 HIGH
- **Description:** Ivanti Connect Secure and Ivanti Policy Secure Privilege Escalation Vulnerability
- **Affected Versions:**
  - Pulse Connect Secure: Version 9.x and 22.x
  - Pulse Policy Secure: Version 9.x and 22.x
  - ZTA Gateways: Version 9.x and 22.x

CVE-2024-21893: Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons' SAML component, allows remote attackers to perform SSRF attacks using insufficient validation of user-supplied information. Attackers can persuade the application to communicate with another system with a specially crafted request and access sensitive data on the local network.

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N ⇒ **Base Score:** 8.2 HIGH
- **Description:** Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability
- **Affected Versions:**
  - Pulse Connect Secure: Version 9.x and 22.x
  - Pulse Policy Secure: Version 9.x and 22.x
  - ZTA Gateways: Version 9.x and 22.x

Attack Models and Potential Impact

CVE-2024-21888 Details:

- **Attack Model:**
  - Threat actors can exploit this vulnerability by sending a specially crafted request to the affected software or web application. The attacker can then execute arbitrary code on the target system with the privileges of the affected software or web application. This vulnerability allows the user to elevate their privileges to administrator privileges
- **Potential Impact:**
  - Based on available information, this vulnerability could allow a user to obtain administrative privileges, potentially leading to unauthorized access and control over sensitive information and system resources.

CVE-2024-21893 Details:

- **Attack Model:**
  - CVE-2024-21893 is a server-side request forgery (SSRF) vulnerability in the SAML component. This vulnerability allows an unauthenticated threat actor to access restricted resources without authentication.
- **Potential Impact:**
  - Based on available information, this vulnerability could allow an attacker to access certain restricted resources without authentication, potentially leading to unauthorized access to sensitive information and system resources.

Indicators of Compromise (IOCs)

The IOCs in the "Investigating Ivanti Connect Secure VPN Zero-Day Exploitation" report published by Mandiant on February 2, 2024 are as follows.

IP Addresses:

- 146.0.228[.]66
- 159.65.130[.]146
- 8.137.112[.]245
- 91.92.254[.]14
- 186.179.39[.]235
- 50.215.39[.]49
- 45.61.136[.]14
- 173.220.106[.]166

Domains:

- symantke[.]com
- miltonhouse[.]nl
- entraide-internationale[.]fr
- api.d-n-s[.]name
- cpanel.netbar[.]org
- clickcom[.]click
- clicko[.]click
- duorhytm[.]fun
- line-api[.]com
- areekaweb[.]com
- ehangmun[.]com
- secure-cama[.]com

Filenames:

- logo.gif
- login.gif
- [a-fA-F0-9]{10}\.css
- visits.py

Hashes:

- **MD5**: 3045f5b3d355a9ab26ab6f44cc831a83
- **MD5**: 3d97f55a03ceb4f71671aa2ecf5b24e9
- **MD5**: 2ec505088b942c234f39a37188e80d7a
- **MD5**: 8eb042da6ba683ef1bae460af103cc44
- **MD5**: a739bd4c2b9f3679f43579711448786f
- **MD5**: a81813f70151a022ea1065b7f4d6b5ab
- **MD5**: d0c7a334a4d9dcd3c6335ae13bee59ea
- **MD5**: e8489983d73ed30a4240a14b1f161254
- **MD5**: 465600cece80861497e8c1c86a07a23e

Conclusion and Recommendation

Ivanti has released new security patches as of January 31st. Applying these patches quickly will reduce the likelihood of organizations being affected by vulnerabilities and protect data integrity.