



# NCSC-2024-0442

## Kwetsbaarheden verholpen in Ivanti Connect Secure en Policy Secure

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-11-2024

### **TLP:WHITE**

#### **Toegestane verspreiding van TLP:WHITE**

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First ([www.first.org/tlp](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

Feiten

Ivanti heeft kwetsbaarheden verholpen in Connect Secure en Policy Secure.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Cross-Site Scripting (XSS)
- Verhoogde gebruikersrechten
- (Remote) code execution (Gebruikersrechten)

Om code executie te verkrijgen is voorafgaande authenticatie met admin rechten vereist. Kwetsbaarheid met kenmerk CVE-2024-11004 kan echter misbruikt worden om op afstand zonder authenticatie admin rechten te verkrijgen. Hiervoor moet een gebruiker wel met admin rechten verleid worden om een malafide webpagina te openen.

Oplossingen

Ivanti heeft fixes uitgebracht om de kwetsbaarheid te verhelpen voor versies Connect Secure versie 22.7R2.3 en Policy Secure 22.7R1.2. Zie de referentie voor meer informatie.

Referenties

➤ <https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs>

Kwetsbaarheden

| CVE              | CVSS Score   |
|------------------|--------------|
| ➤ CVE-2024-8495  | 7.5 HIGH     |
| ➤ CVE-2024-9420  | 8.8 HIGH     |
| ➤ CVE-2024-11004 | 8.4 HIGH     |
| ➤ CVE-2024-11005 | 9.1 CRITICAL |

|                  |              |
|------------------|--------------|
| > CVE-2024-11006 | 9.1 CRITICAL |
| > CVE-2024-11007 | 9.1 CRITICAL |
| > CVE-2024-37400 |              |
| > CVE-2024-38649 |              |
| > CVE-2024-38655 |              |
| > CVE-2024-38656 |              |
| > CVE-2024-39709 |              |
| > CVE-2024-39710 |              |
| > CVE-2024-39711 |              |
| > CVE-2024-39712 |              |
| > CVE-2024-47905 | 4.9 MEDIUM   |
| > CVE-2024-47906 | 7.8 HIGH     |
| > CVE-2024-47907 | 7.5 HIGH     |
| > CVE-2024-47909 | 4.9 MEDIUM   |

CWE's

| CWE       | Beschrijving                                          |
|-----------|-------------------------------------------------------|
| > CVE-267 | Privilege Defined With Unsafe Actions                 |
| > CVE-126 | Buffer Over-read                                      |
| > CVE-732 | Incorrect Permission Assignment for Critical Resource |
| > CVE-426 | Untrusted Search Path                                 |
| > CVE-416 | Use After Free                                        |
| > CVE-476 | NULL Pointer Dereference                              |

|                           |                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------|
| ➤ <a href="#">CWE-78</a>  | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| ➤ <a href="#">CWE-121</a> | Stack-based Buffer Overflow                                                                |
| ➤ <a href="#">CWE-79</a>  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')       |
| ➤ <a href="#">CWE-125</a> | Out-of-bounds Read                                                                         |
| ➤ <a href="#">CWE-787</a> | Out-of-bounds Write                                                                        |
| ➤ <a href="#">CWE-276</a> | Incorrect Default Permissions                                                              |

Getroffen producten

|                |
|----------------|
| <b>ivanti</b>  |
| connect_secure |
| policy_secure  |

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.