Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# 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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

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

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

## Getroffen producten

| **ivanti** |
|---|
| connect_secure |
| policy_secure |

## Disclaimer