Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0416 revisie 1.0.1

PRIORITEIT: HOOG

ZeroDay kwetsbaarheden verholpen in Ivanti Connect Secure

Publicatiedatum: 03-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Update Revisie

Ivanti heeft twee nieuwe kwetsbaarheden gepubliceerd (CVE-2026-111357 en CVE-2026-118527), die samen met CVE-2026-104935 actief zijn misbruikt.

Naast de toevoeging van deze twee kwetsbaarheden is ook de lijst met kwetsbare versies uitgebreid. Zo zijn versies 25.1.1.2 en 22.8R2.5, die eerder als gepatcht werden beschouwd voor CVE-2026-104935, nog kwetsbaar voor CVE-2026-111357 en CVE-2026-118527.

Feiten

Ivanti heeft meerdere kwetsbaarheden verholpen in Connect Secure.

Duiding

Een kwaadwillende kan de kwetsbaarheid (CVE-2026-104935) misbruiken om zonder voorafgaande authenticatie willekeurige commando's uit te voeren op het kwetsbare systeem.

Ivanti meldt op de hoogte te zijn van rapporten dat de kwetsbaarheid als ZeroDay kwetsbaarheid is misbruikt. Er is (nog) geen publieke Proof-of-Concept (PoC) beschikbaar, maar het NCSC verwacht dat publieke PoC of exploitcode op korte termijn beschikbaar komt, wat de kans op grootschalig misbruik vergroot.

**Update: **Ivanti heeft twee nieuwe kwetsbaarheden gepubliceerd (CVE-2026-111357 en CVE-2026-118527), die samen met CVE-2026-104935 actief zijn misbruikt.

Naast de toevoeging van deze twee kwetsbaarheden is ook de lijst met kwetsbare versies uitgebreid. Zo is versie 25.1.1.2, die eerder als gepatcht werd beschouwd voor CVE-2026-104935, nog kwetsbaar voor CVE-2026-111357 en CVE-2026-118527.

Oplossingen

Ivanti heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-104935	10.0 CRITICAL
CVE-2026-111357	7.0 HIGH
CVE-2026-118527	

CWE's

CWE	Beschrijving
CWE-290	Authentication Bypass by Spoofing

Getroffen producten

Ivanti
Connect 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.