Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0180

Kwetsbaarheden verholpen in Ivanti Sentry

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 10-06-2026
Revisie: 1.0.1

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

Update Revisie 1

Er is een gedetailleerde blogpost gepubliceerd waarin de kwetsbaarheden in detail worden uitgelegd. Ook is inmiddels bekend dat de Ivanti Sentry via de Ivanti EPMM bereikt kan worden. De publicatie van deze blogpost vergroot de kans op misbruik.

Feiten

Ivanti heeft twee kwetsbaarheden verholpen in Sentry.

Duiding

Middels de eerste kwetsbaarheid, die Ivanti een CVSS score van 10 geeft, kan een ongeauthenticeerde kwaadwillende op afstand willekeurige code uitvoeren met root rechten. De tweede kwetsbaarheid, met volgens Ivanti een CVSS score van 9.9, kan door een ongeauthenticeerde kwaadwillende op afstand worden misbruikt om administratieve accounts aan te maken.

Misbruik van deze kwetsbaarheid is mogelijk via het Ivanti EPMM systeem behorende bij het kwetsbare Ivanti Sentry systeem.

De kwetsbaarheden hebben Ivanti bereikt via responsible disclosure. Momenteel vind er - voor zover bekend - geen actief misbruik van deze kwetsbaarheden plaats en is geen publieke PoC code beschikbaar. Het NCSC verwacht echter dat dit op korte termijn zal volgen.

Oplossingen

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

Dreigingsinformatie

Er is een gedetailleerde blogpost gepubliceerd waarin de kwetsbaarheden in detail worden uitgelegd. De publicatie van deze blogpost vergroot de kans op misbruik. Zie de blog van Watchtwr: https://labs.watchtowr.com/more-evidence-that-words-dont-mean-what-we-thought-they-meant-ivanti-sentry-pre-auth-os-command-injection-cve-2026-10520/

Referenties

- https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-10520-CVE-2026-10523?language=en_US

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-10523	9.9 CRITICAL
CVE-2026-10520	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Getroffen producten

Ivanti
Sentry

Disclaimer