



NCSC-2026-0059

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-03-2026

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

CISA heeft de kwetsbaarheid met kenmerk CVE-2026-1603 op de KEV-lijst geplaatst.

Feiten

Ivanti heeft kwetsbaarheden verholpen in Ivanti Endpoint Manager (Specifiek voor versies vóór 2024 SU5).

Duiding

De kwetsbaarheid met kenmerk CVE-2026-1603 betreft een authenticatie-bypass die het mogelijk maakt voor externe, niet-geauthenticeerde aanvallers om toegang te krijgen tot bepaalde opgeslagen inloggegevens, wat kan leiden tot compromittering van gevoelige data. De kwetsbaarheid met kenmerk CVE-2026-1602 betreft een SQL-injectie die het mogelijk maakt voor externe, geauthenticeerde aanvallers om willekeurige SQL-query's uit te voeren, wat kan leiden tot ongeautoriseerde toegang tot gevoelige database-informatie. Beide kwetsbaarheden kunnen de integriteit en vertrouwelijkheid van de gegevens in het systeem in gevaar brengen.

Van de kwetsbaarheid met kenmerk CVE-2026-1603 meldt het Amerikaanse CISA dat deze binnen een Amerikaanse overheidsorganisatie is misbruikt. Verdere details zijn niet vrijgegeven en er is (nog) geen publieke Proof-of-Concept-code of exploit bekend.

Oplossingen

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

Referenties

- https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-1603

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-1603	8.6 HIGH
➤ CVE-2026-1602	6.5 MEDIUM

CWE's

CWE	Beschrijving
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CWE-288	Authentication Bypass Using an Alternate Path or Channel

Getroffen producten

Ivanti
Endpoint Manager

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.