



NCSC-2025-0391

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-12-2025

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 Ivanti Endpoint Manager (Specifiek voor versies vóór 2024 SU4 SR1).

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van Ivanti Endpoint Manager. De eerste kwetsbaarheid betreft een opgeslagen XSS-kwetsbaarheid die het mogelijk maakt voor ongeauthenticeerde aanvallers om willekeurige JavaScript-code uit te voeren in de context van een beheerderssessie, wat kan leiden tot ongeautoriseerde acties binnen de applicatie. Een tweede kwetsbaarheid stelt aanvallers in staat om willekeurige bestanden op de server te schrijven, wat mogelijk kan leiden tot externe code-uitvoering, hoewel dit ook gebruikersinteractie vereist. Daarnaast is er een pad-traversal-kwetsbaarheid die het voor geauthenticeerde aanvallers mogelijk maakt om bestanden buiten de bedoelde directory te schrijven, wat kan leiden tot verdere beveiligingsinbreuken of dataintegriteitsproblemen. Tot slot heeft de patchmanagementcomponent een kwetsbaarheid die ongeauthenticeerde aanvallers in staat stelt om willekeurige code uit te voeren, wat kan resulteren in ongeautoriseerde toegang of controle over de getroffen systemen.

Oplossingen

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

Referenties

➤ <https://forums.ivanti.com/s/article/Security-Advisory-EPM-December-2025-for-EPM-2024>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-10573	9.6 CRITICAL
➤ CVE-2025-13659	8.8 HIGH
➤ CVE-2025-13661	7.1 HIGH
➤ CVE-2025-13662	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-347	Improper Verification of Cryptographic Signature
> CWE-913	Improper Control of Dynamically-Managed Code Resources

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.