Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0318

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-10-2025

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.

Duiding

De kwetsbaarheden omvatten een onveilige deserialisatie, een pad-traversal en meerdere SQL-injectie kwetsbaarheden. De onveilige deserialisatie kan door lokale, geauthenticeerde aanvallers worden misbruikt om verhoogde privileges te verkrijgen, wat leidt tot ongeautoriseerde toegang tot gevoelige functionaliteiten en gegevens binnen het systeem. De pad-traversal kwetsbaarheid stelt externe, ongeauthenticeerde aanvallers in staat om willekeurige code uit te voeren op getroffen systemen, wat kan resulteren in ongeautoriseerde toegang en controle over het systeem. De SQL-injectie kwetsbaarheden stellen geauthenticeerde aanvallers in staat om willekeurige SQL-query's tegen de database uit te voeren, wat kan leiden tot ongeautoriseerde toegang tot gevoelige gegevens en compromittering van de integriteit en vertrouwelijkheid van opgeslagen informatie.

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-Ivanti-Endpoint-Manager-EPM-October-2025

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-11622	8.5 HIGH
CVE-2025-9713	5.3 MEDIUM
CVE-2025-11623	5.3 MEDIUM
CVE-2025-62392	5.3 MEDIUM
CVE-2025-62390	5.3 MEDIUM
CVE-2025-62389	5.3 MEDIUM

CVE-2025-62388	**5.3 MEDIUM**
CVE-2025-62387	**5.3 MEDIUM**
CVE-2025-62385	**5.3 MEDIUM**
CVE-2025-62391	**5.3 MEDIUM**
CVE-2025-62383	**5.3 MEDIUM**
CVE-2025-62386	**5.3 MEDIUM**
CVE-2025-62384	**5.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Ivanti
Endpoint Manager

Disclaimer