Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0017

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-01-2025

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 (EPM) die aanwezig waren in versies vóór de januari 2025 beveiligingsupdates.

Duiding

De kwetsbaarheden omvatten path traversal, SQL-injectie, deserialisatie, onjuist bestandsnaamvalidatie en onvoldoende validatie van handtekeningen. Deze kwetsbaarheden stellen zowel ongeauthenticeerde als geauthenticeerde aanvallers in staat om toegang te krijgen tot gevoelige informatie, code op afstand uit te voeren, en kunnen leiden tot een Denial-of-Service.

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-January-2025-for-EPM-2024-and-EPM-2022-SU6

Kwetsbaarheden

CVE	CVSS Score
› CVE-2024-10811	9.8 CRITICAL
› CVE-2024-13158	7.2 HIGH
› CVE-2024-13159	9.8 CRITICAL
› CVE-2024-13160	9.8 CRITICAL
› CVE-2024-13161	9.8 CRITICAL
› CVE-2024-13162	7.2 HIGH
› CVE-2024-13163	7.8 HIGH

CVE-2024-13164	7.8 HIGH
CVE-2024-13165	7.5 HIGH
CVE-2024-13166	7.5 HIGH
CVE-2024-13167	7.5 HIGH
CVE-2024-13168	7.5 HIGH
CVE-2024-13169	7.8 HIGH
CVE-2024-13170	7.5 HIGH
CVE-2024-13171	7.8 HIGH
CVE-2024-13172	7.8 HIGH
CVE-2024-32848	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-918	Server-Side Request Forgery (SSRF)
CWE-347	Improper Verification of Cryptographic Signature
CWE-908	Use of Uninitialized Resource
CWE-36	Absolute Path Traversal
CWE-426	Untrusted Search Path
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-125	Out-of-bounds Read
CWE-502	Deserialization of Untrusted Data

CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-787	Out-of-bounds Write
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

ivanti
endpoint_manager
epm
ivanti_endpoint_manager__2022_su6
ivanti_endpoint_manager__2024_security_patch
ivanti_endpoint_manager__2024_su1

Disclaimer