Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0369

Kwetsbaarheden verholpen in Ivanti Endpoint Manager

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-09-2024
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

New revision

Feiten

Ivanti heeft kwetsbaarheden verholpen in Ivanti Endpoint Manager.

Duiding

Er zijn kwetsbaarheden verholpen in Ivanti Endpoint Manager. Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- (Remote) code execution (Administrator/Root rechten)
- Toegang tot systeemgegevens
- Verhoogde gebruikersrechten

Ivanti heeft geen aanwijzingen dat er actief misbruik plaatsvindt van deze kwetsbaarheden.

Onderzoekers hebben Proof-of-Concept-code gepubliceerd, waarmee de kwetsbaarheid met kenmerk CVE-2024-29847 kan worden aangetoond. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheeromgeving.

Oplossingen

Ivanti heeft updates uitgebracht om de kwetsbaarheden in Ivanti Endpoint Manager te verhelpen. Zie de referentie voor meer informatie.

Referenties

- https://forums.ivanti.com/s/article/Security-Advisory-EPM-September-2024-for-EPM-2024-and-EPM-2022

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-8191	9.8 CRITICAL

CVE-2024-8320	5.3 MEDIUM
CVE-2024-8321	8.6 HIGH
CVE-2024-8322	8.8 HIGH
CVE-2024-8441	6.7 MEDIUM
CVE-2024-29847	
CVE-2024-32840	7.2 HIGH
CVE-2024-32842	7.2 HIGH
CVE-2024-32843	7.2 HIGH
CVE-2024-32845	7.2 HIGH
CVE-2024-32846	7.2 HIGH
CVE-2024-32848	7.2 HIGH
CVE-2024-34779	7.2 HIGH
CVE-2024-34783	7.2 HIGH
CVE-2024-34785	7.2 HIGH
CVE-2024-37397	8.2 HIGH

CWE's

CWE	Beschrijving
CWE-1390	Weak Authentication
CWE-306	Missing Authentication for Critical Function
CWE-427	Uncontrolled Search Path Element
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-611	Improper Restriction of XML External Entity Reference

CWE-502	Deserialization of Untrusted Data

Getroffen producten

ivanti
endpoint_manager

Disclaimer