Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0399

Kwetsbaarheden verholpen in Ivanti Cloud Services Appliance

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-10-2024

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 drie kwetsbaarheden verholpen in Cloud Services Appliance.

Duiding

Een geauthenticeerde kwaadwillende die reeds admin rechten bezit kan de kwetsbaarheden misbruiken om op afstand code en SQL statements uit te voeren, of middels path traversal restricties te omzeilen.

Ivanti geeft aan bij gebruikers van versie 4.6 met patch 518 en lager, beperkte exploitatie van CVE-2024-9379 en CVE-2024-9380 in combinatie met CVE-2024-8963 te hebben waargenomen. Kwetsbaarheid CVE-2024-8963 is in latere versies verholpen en Ivanti heeft geen exploitatie waargenomen bij gebruikers vanaf versie 5.0.

Oplossingen

Ivanti heeft versie 5.0.2 uitgebracht om de kwetsbaarheden te verhelpen.

Referenties

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-9381	
CVE-2024-9380	
CVE-2024-9379	

CWE's

CWE	Beschrijving
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

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

Getroffen producten

ivanti
cloud_services_appliance
endpoint_manager_cloud_services_appliance

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.