Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0379

Kwetsbaarheden verholpen in Ivanti Cloud Services Appliance

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 20-09-2024

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 kwetsbaarheden verholpen in Cloud Services Appliance v 4.6.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om via een path-traversal een command-injection uit te voeren, waardoor het systeem zonder voorafgaande authenticatie kan worden bediend en mogelijk overgenomen. Ivanti geeft aan informatie te hebben dat de kwetsbaarheden bij een kleine groep klanten is misbruikt. Ook het Amerikaanse CISA meldt via de Known Exploited Vulnerability Database dat de kwetsbaarheden gericht zijn misbruikt.

Systemen die, tegen het advies van Ivanti in, geïmplementeerd zijn als Single-home systeem, ofwel waar eth0 zowel het interne als het externe netwerk bedient, lopen verhoogd risico tot misbruik.

CSA 4.6 is End-of-Life. Gebruikers van CSA die inmiddels overgegaan zijn naar CSA 5 zijn NIET kwetsbaar. In tegenstelling tot het standaard beleid van Ivanti, heeft Ivanti alsnog gekozen om updates uit te brengen om deze kwetsbaarheden te verhelpen in het EOL v 4.6.

Oplossingen

Ivanti heeft alsnog gekozen om een update uit te brengen om de kwetsbaarheden te verhelpen in v4.6 Patch 519. Het NCSC wijst er echter wel op dat v 4.6 van de Cloud Services Appliance sinds juni 2024 End-of-Life is en geen updates meer heeft ontvangen, met uitzondering van deze. Het is daarom aan te raden de verouderde systeem te vervangen voor een nieuwer, ondersteund systeem, versie 5 of hoger.

Zie verder de bijgevoegde referenties voor meer informatie.

Dreigingsinformatie

Gebruikers van CSA v4.6 (Patch 518 en lager) kunnen controleren of een systeem is gecompromitteerd, door te controleren of er lokaal gebruikers zijn aangemaakt met administrator-rechten.

Referenties

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Service-Appliance-CSA-CVE-2024-8190
- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-4-6-Cloud-Services-Appliance-CVE-2024-8963

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-8190	7.2 HIGH
CVE-2024-8963	

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Getroffen producten

ivanti
csa
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.