Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0379

Kwetsbaarheden verholpen in Ivanti Cloud Services Appliance

2024-09-20 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Ivanti heeft kwetsbaarheden verholpen in Cloud Services Appliance v 4.6.

Interpretaties

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