Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0276

Kwetsbaarheden verholpen in Splunk

2024-07-02 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

De ontwikkelaars van Splunk hebben kwetsbaarheden verholpen in Splunk en Splunk Enterprise.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, willekeurige code uit te (laten) voeren middels Command-injection, of om een Cross-Site-Scripting-aanval uit te voeren. Een dergelijke aanval kan leiden tot uitvoer van willekeurige code in de browser van het slachtoffer, of toegang tot gevoelige gegevens in de context van de browser van het slachtoffer.

Oplossingen

Splunk heeft updates uitgebracht voor Splunk en Splunk Enterprise. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://advisory.splunk.com/advisories/SVD-2024-0702
- https://advisory.splunk.com/advisories/SVD-2024-0703
- https://advisory.splunk.com/advisories/SVD-2024-0704
- https://advisory.splunk.com/advisories/SVD-2024-0705
- https://advisory.splunk.com/advisories/SVD-2024-0706
- https://advisory.splunk.com/advisories/SVD-2024-0707
- https://advisory.splunk.com/advisories/SVD-2024-0709
- https://advisory.splunk.com/advisories/SVD-2024-0710
- https://advisory.splunk.com/advisories/SVD-2024-0711
- https://advisory.splunk.com/advisories/SVD-2024-0712
- https://advisory.splunk.com/advisories/SVD-2024-0713
- https://advisory.splunk.com/advisories/SVD-2024-0714
- https://advisory.splunk.com/advisories/SVD-2024-0715
- https://advisory.splunk.com/advisories/SVD-2024-0716
- https://advisory.splunk.com/advisories/SVD-2024-0717