Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0381

Kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-12-2025

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

Splunk heeft kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform.

Duiding

De kwetsbaarheden omvatten verschillende problemen, waaronder de mogelijkheid voor laaggeprivilegieerde gebruikers om ongeautoriseerde dashboards te creëren, toegang te krijgen tot gevoelige informatie via mobiele meldingen, en de injectie van ANSI-escape codes in logbestanden. Daarnaast kunnen hooggeprivilegieerde gebruikers ongeautoriseerde JavaScript-code uitvoeren, en zijn er problemen met onjuiste machtigingen die niet-beheerders toegang geven tot installatiebestanden. Deze kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang tot gevoelige gegevens en verstoringen van de applicatiefuncties, wat de integriteit en beschikbaarheid van de systemen in gevaar brengt.

Oplossingen

Splunk heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://advisory.splunk.com//advisories/SVD-2025-1201
- https://advisory.splunk.com//advisories/SVD-2025-1202
- https://advisory.splunk.com//advisories/SVD-2025-1203
- https://advisory.splunk.com//advisories/SVD-2025-1204
- https://advisory.splunk.com//advisories/SVD-2025-1205
- https://advisory.splunk.com//advisories/SVD-2025-1206
- https://advisory.splunk.com//advisories/SVD-2025-1207
- https://advisory.splunk.com//advisories/SVD-2025-1208

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-20382	**5.1 MEDIUM**
CVE-2025-20383	**5.3 MEDIUM**
CVE-2025-20384	**6.9 MEDIUM**

CVE-2025-20385	4.8 MEDIUM
CVE-2025-20386	8.6 HIGH
CVE-2025-20387	8.7 HIGH
CVE-2025-20388	5.1 MEDIUM
CVE-2025-20389	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-117	Improper Output Neutralization for Logs
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-404	Improper Resource Shutdown or Release
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Splunk
Splunk Cloud Platform
Splunk Enterprise
Splunk Secure Gateway

Disclaimer