



NCSC-2025-0099

Kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 27-03-2025

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 stellen laaggeprivilegieerde gebruikers in staat om hogere gebruikersrechten te misbruiken, wat kan leiden tot ongeautoriseerde acties en toegang tot gevoelige informatie. Dit kan gebeuren via phishing-aanvallen en Cross-Site Request Forgery (CSRF) aanvallen, wat de integriteit en vertrouwelijkheid van gegevens in gevaar kan brengen. De kwetsbaarheden omvatten ook ongeautoriseerde bestandsuploads en onjuiste toegang tot gegevens in KVStore-collecties, wat kan resulteren in ongeautoriseerde wijzigingen aan gevoelige data.

Oplossingen

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

Referenties

- <https://advisory.splunk.com/advisories/SVD-2025-0301>
- <https://advisory.splunk.com/advisories/SVD-2025-0302>
- <https://advisory.splunk.com/advisories/SVD-2025-0303>
- <https://advisory.splunk.com/advisories/SVD-2025-0304>
- <https://advisory.splunk.com/advisories/SVD-2025-0305>
- <https://advisory.splunk.com/advisories/SVD-2025-0306>
- <https://advisory.splunk.com/advisories/SVD-2025-0307>
- <https://advisory.splunk.com/advisories/SVD-2025-0310>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-20226	5.1 MEDIUM
➤ CVE-2025-20227	5.3 MEDIUM
➤ CVE-2025-20228	5.3 MEDIUM
➤ CVE-2025-20229	8.7 HIGH

> CVE-2025-20230	5.3 MEDIUM
> CVE-2025-20231	2.1 LOW
> CVE-2025-20232	5.1 MEDIUM
> CVE-2025-20233	2.0 LOW

CWE's

CWE	Beschrijving
> CWE-732	Incorrect Permission Assignment for Critical Resource
> CWE-532	Insertion of Sensitive Information into Log File
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-284	Improper Access Control
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-20	Improper Input Validation

Getroffen producten

Splunk
Splunk Enterprise
Splunk Cloud Platform
Splunk Secure Gateway
splunk

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.