



NCSC-2025-0212

Kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 08-07-2025

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 in Splunk Enterprise en Splunk Cloud Platform stellen zowel low-privileged als high-privileged gebruikers in staat om ongeautoriseerde acties uit te voeren, zoals het onderdrukken van waarschuwingen, het uitvoeren van externe commando's, en het veroorzaken van een denial-of-service. Daarnaast kunnen ongeauthenticeerde aanvallers kwetsbaarheden misbruiken om wijzigingen aan te brengen in de lidmaatschapsconfiguraties van een Splunk Search Head Cluster of om gevoelige informatie bloot te stellen. De exploitatie van deze kwetsbaarheden vereist vaak sociale-engineeringtechnieken, wat de noodzaak van waakzaamheid onder gebruikers benadrukt.

Oplossingen

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

Referenties

- <https://advisory.splunk.com//advisories/SVD-2025-0702>
- <https://advisory.splunk.com//advisories/SVD-2025-0703>
- <https://advisory.splunk.com//advisories/SVD-2025-0704>
- <https://advisory.splunk.com//advisories/SVD-2025-0705>
- <https://advisory.splunk.com//advisories/SVD-2025-0706>
- <https://advisory.splunk.com//advisories/SVD-2025-0707>
- <https://advisory.splunk.com//advisories/SVD-2025-0708>
- <https://advisory.splunk.com//advisories/SVD-2025-0709>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-20300	4.3 MEDIUM
➤ CVE-2025-20319	6.8 MEDIUM
➤ CVE-2025-20320	6.3 MEDIUM

> CVE-2025-20321	6.5 MEDIUM
> CVE-2025-20322	4.3 MEDIUM
> CVE-2025-20323	4.3 MEDIUM
> CVE-2025-20324	5.4 MEDIUM
> CVE-2025-20325	3.1 LOW

CWE's

CWE	Beschrijving
> CWE-35	Path Traversal: '.../.../'
> CWE-352	Cross-Site Request Forgery (CSRF)
> CWE-284	Improper Access Control
> CWE-863	Incorrect Authorization
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Splunk
Splunk Enterprise

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.