



Advisory NCSC-2026-0457

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Splunk Enterprise

Publicatiedatum: 28-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Splunk heeft meerdere kwetsbaarheden verholpen in Splunk Enterprise.

Duiding

In Splunk Enterprise zijn verschillende kwetsbaarheden aanwezig in versies eerder dan 10.4.4 (en enkele andere specifieke versies). Deze omvatten onder andere:

- onjuiste verificatie in de Data Management REST API waardoor gebruikers met bepaalde rollen toegang kunnen krijgen tot of verwijderen van SPL2 preview jobs en resultaten die zij niet bezitten
- onvoldoende limieten in request-header parsing in de JavaScript logger endpoint die een Denial-of-Service (DoS) kan veroorzaken
- misbruik van de REST API voor lookup table files door niet-admin gebruikers om DoS te veroorzaken
- onvoldoende toegangscontrole op de Edge Processor package download endpoint waardoor ongeauthenticeerde gebruikers overmatig resourcegebruik kunnen veroorzaken
- het uitvoeren van potentieel gevaarlijke SPL-commando's door gebruikers met `schedule_search` capability
- toegang tot mobiele alert notificatiegegevens door laaggeprivilegieerde gebruikers via onvoldoende autorisatie in App Key Value Store REST API
- uitvoering van willekeurige OS-commando's via onvoldoende restricties in Splunk Web Manager XML configuratie
- onbevoegde verplaatsing van field extractions of transformations naar niet-toegestane applicaties
- omzeilen van filterrestricties door gebruikers zonder admin of power rol via onjuiste verwerking van speciale karakters
- onbevoegde aanpassingen van sourcetype renaming configuraties
- uitschakeling van federated search providers door phishing van gebruikers met `edit_federated_providers` capability
- het afleiden van de PostgreSQL sidecar database superuser wachtwoord door niet-admin gebruikers via blootstelling in zoekjob logs.

Oplossingen

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

Referenties

- <https://advisory.splunk.com/advisories/SVD-2026-1007>
- <https://advisory.splunk.com/advisories/SVD-2026-1008>
- <https://advisory.splunk.com/advisories/SVD-2026-1010>
- <https://advisory.splunk.com/advisories/SVD-2026-1011>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76287	5.4 MEDIUM
CVE-2026-76288	7.5 HIGH
CVE-2026-76289	6.5 MEDIUM
CVE-2026-76290	7.5 HIGH
CVE-2026-76291	8.8 HIGH
CVE-2026-76292	6.5 MEDIUM
CVE-2026-76293	7.2 HIGH
CVE-2026-76294	4.3 MEDIUM
CVE-2026-76295	4.3 MEDIUM
CVE-2026-76296	4.3 MEDIUM
CVE-2026-76297	4.2 MEDIUM
CVE-2026-76298	8.8 HIGH
CVE-2026-76299	9.9 CRITICAL
CVE-2026-76300	8.8 HIGH
CVE-2026-76301	9.8 CRITICAL
CVE-2026-76302	9.9 CRITICAL

CVE	CVSS Score
CVE-2026-76303	5.7 MEDIUM
CVE-2026-76304	4.3 MEDIUM
CVE-2026-76305	6.5 MEDIUM
CVE-2026-76306	7.5 HIGH
CVE-2026-76307	7.2 HIGH
CVE-2026-76308	6.5 MEDIUM
CVE-2026-76406	5.9 MEDIUM
CVE-2026-76407	
CVE-2026-76408	
CVE-2026-76526	8.8 HIGH
CVE-2026-76527	
CVE-2026-76528	
CVE-2026-76529	
CVE-2026-76530	8.8 HIGH
CVE-2026-76531	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-203	Observable Discrepancy
CWE-321	Use of Hard-coded Cryptographic Key
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-424	Improper Protection of Alternate Path
CWE-552	Files or Directories Accessible to External Parties
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-647	Use of Non-Canonical URL Paths for Authorization Decisions

CWE	Beschrijving
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-862	Missing Authorization
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

Splunk
Splunk Enterprise
Splunk Secure Gateway

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 or 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.