Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0322

Kwetsbaarheden verholpen in Splunk Enterprise door Splunk

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-08-2026

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 meerdere kwetsbaarheden verholpen in Splunk Enterprise, specifiek in versies vóór 10.4.2, 10.2.6, 10.0.9 en 9.4.14.

Duiding

De kwetsbaarheden in Splunk Enterprise betreffen onder andere:

- Onvoldoende handhaving van authenticatie- en autorisatiecontroles in REST API's, waardoor niet-bevoegde gebruikers toegang kunnen krijgen tot gevoelige data, configuraties en kunnen leiden tot het uitvoeren van willekeurige SPL-commando's met verhoogde privileges.
- Meerdere kwetsbaarheden die Cross-Site Scripting (XSS) mogelijk maken, waarbij kwaadwillenden via speciaal vervaardigde links of content JavaScript kunnen injecteren en uitvoeren in de context van andere gebruikers.
- Verder kunnen niet-geauthenticeerde of laaggeprivilegieerde gebruikers via diverse componenten zoals Dataset Explorer, Dashboard Studio, Search Head Cluster, en andere interfaces, commando's uitvoeren, bestanden manipuleren, of configuraties wijzigen.
- Sommige kwetsbaarheden maken het mogelijk om sessiegegevens te benaderen, authenticatietokens te onderscheppen, of administratieve sessies te forceren. Exploitatie kan plaatsvinden via phishing, het openen van kwaadaardige links, of misbruik van onvoldoende beveiligde API-eindpunten.

De kwetsbaarheden beïnvloeden verschillende onderdelen zoals de REST API, Splunk Web Manager, Dashboard Studio, federated search, en de Edge Processor component. De impact omvat ongeautoriseerde toegang tot data, manipulatie van systeemconfiguraties, uitvoering van code met verhoogde rechten, en mogelijke verstoring van de beschikbaarheid van de dienst.

Naast de genoemde kwetsbaarheden heeft Splunk ook updates uitgebracht om kwetsbaarheden in Third-Party producten waarvan Splunk gebruik maakt verholpen. Van deze kwetsbaarheden zijn eerder updates uitgebracht die Splunk nu verwerkt heeft in de eigen software stack.

Oplossingen

Splunk heeft updates uitgebracht om de kwetsbaarheden in Splunk Enterprise te verhelpen. Naast de inzet van deze updates is voor twee kwetsbaarheden nog een additionele, handmatige actie nodig. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://advisory.splunk.com/advisories/SVD-2026-0801
- https://advisory.splunk.com/advisories/SVD-2026-0802

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76251	7.1 HIGH
CVE-2026-76252	6.8 MEDIUM
CVE-2026-76253	8.8 HIGH
CVE-2026-76254	7.5 HIGH
CVE-2026-76255	6.4 MEDIUM
CVE-2026-76256	4.3 MEDIUM
CVE-2026-76257	6.5 MEDIUM
CVE-2026-76258	6.5 MEDIUM
CVE-2026-76259	8.8 HIGH
CVE-2026-76260	6.5 MEDIUM
CVE-2026-76261	5.3 MEDIUM
CVE-2026-76262	7.5 HIGH
CVE-2026-76263	5.4 MEDIUM
CVE-2026-76309	4.3 MEDIUM
CVE-2026-76310	9.4 CRITICAL
CVE-2026-76311	9.4 CRITICAL
CVE-2026-76312	9.4 CRITICAL
CVE-2026-76313	8.8 HIGH
CVE-2026-76314	8.8 HIGH
CVE-2026-76315	8.8 HIGH
CVE-2026-76316	8.8 HIGH

CVE-2026-76317	8.8 HIGH
CVE-2026-76318	5.7 MEDIUM
CVE-2026-76319	8.8 HIGH
CVE-2026-76320	5.9 MEDIUM
CVE-2026-76321	7.3 HIGH
CVE-2026-76322	6.7 MEDIUM
CVE-2026-76323	6.4 MEDIUM
CVE-2026-76324	5.7 MEDIUM
CVE-2026-76325	7.3 HIGH
CVE-2026-76326	5.7 MEDIUM
CVE-2026-76327	6.4 MEDIUM
CVE-2026-76328	6.7 MEDIUM
CVE-2026-76329	6.4 MEDIUM
CVE-2026-76330	7.1 HIGH
CVE-2026-76331	8.1 HIGH
CVE-2026-76332	7.1 HIGH
CVE-2026-76333	7.1 HIGH
CVE-2026-76334	6.4 MEDIUM
CVE-2026-76335	8.8 HIGH
CVE-2026-76336	7.1 HIGH
CVE-2026-76337	5.3 MEDIUM
CVE-2026-76338	8.1 HIGH
CVE-2026-76339	5.4 MEDIUM

CVE-2026-76340	5.3 MEDIUM
CVE-2026-76341	5.4 MEDIUM
CVE-2026-76342	5.4 MEDIUM
CVE-2026-76343	6.5 MEDIUM
CVE-2026-76344	7.7 HIGH
CVE-2026-76345	6.0 MEDIUM
CVE-2026-76346	5.4 MEDIUM
CVE-2026-76347	5.4 MEDIUM
CVE-2026-76348	3.8 LOW
CVE-2026-76349	6.4 MEDIUM
CVE-2026-76350	8.8 HIGH
CVE-2026-76351	8.8 HIGH
CVE-2026-76352	8.8 HIGH
CVE-2026-76353	5.4 MEDIUM
CVE-2026-76354	8.1 HIGH
CVE-2026-76355	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-24	Path Traversal: '../filedir'
CWE-26	Path Traversal: '/dir/../filename'

CWE-27	Path Traversal: 'dir/../../filename'
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-158	Improper Neutralization of Null Byte or NUL Character
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-269	Improper Privilege Management
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-287	Improper Authentication
CWE-306	Missing Authentication for Critical Function
CWE-321	Use of Hard-coded Cryptographic Key
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

Splunk
Splunk Enterprise
Splunk Secure Gateway

Disclaimer