Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0512

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Splunk Enterprise door Splunk Inc.

Publicatiedatum: 23-11-2026

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 de-len. 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 Inc. heeft meerdere kwetsbaarheden verholpen in Splunk Enterprise.

Duiding

De kwetsbaarheden in Splunk Enterprise betreffen onder andere onjuiste toegangscontrole en onvoldoende validatie in de REST API, het Analytics Workspace component, Classic Dashboards, Data Model Acceleration, en andere onderdelen van het platform.

Hierdoor kunnen gebruikers met beperkte rechten, zoals de 'power' rol of zelfs niet-geauthenticeerde gebruikers, acties uitvoeren die normaal hogere privileges vereisen. Dit omvat het uitvoeren van kwaadaardige SPL-commando's, het manipuleren van private HTML-views, het injecteren van scripts in dashboards en alerts, het verkrijgen van ongeautoriseerde toegang tot gevoelige configuratie- en credentialgegevens, en het veroorzaken van Denial-of-Service door het uitputten van systeembronnen of het laten crashen van processen. Sommige kwetsbaarheden maken gebruik van onjuiste validatie van gebruikersinvoer, onvoldoende neutralisatie van data, of het accepteren van lege gedeelde sleutels in authenticatiemechanismen. Daarnaast kunnen bepaalde kwetsbaarheden leiden tot het persistent blijven van sessies na uitloggen of het creëren van meerdere gebruikersaccounts die naar dezelfde directory verwijzen.

Exploitatie kan plaatsvinden via het misbruiken van API-eindpunten, het openen van kwaadaardige links, of het gebruik van phishingtechnieken om gebruikers te misleiden. De kwetsbaarheden zijn aanwezig in meerdere versies van Splunk Enterprise, met name in versies voorafgaand aan 10.6.1, 10.4.5, 10.2.9, 10.0.12 en 9.4.17.

Oplossingen

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

Referenties

- https://advisory.splunk.com/advisories/SVD-2026-1103

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-131174	5.4 MEDIUM
CVE-2026-131175	7.6 HIGH
CVE-2026-131176	4.3 MEDIUM
CVE-2026-131177	7.1 HIGH
CVE-2026-131178	7.6 HIGH
CVE-2026-131179	7.6 HIGH
CVE-2026-131180	6.3 MEDIUM
CVE-2026-131181	7.1 HIGH
CVE-2026-131182	7.6 HIGH
CVE-2026-131183	5.4 MEDIUM
CVE-2026-131184	6.4 MEDIUM
CVE-2026-131185	6.5 MEDIUM
CVE-2026-131186	6.5 MEDIUM
CVE-2026-131187	4.3 MEDIUM
CVE-2026-131188	7.1 HIGH
CVE-2026-131189	5.3 MEDIUM
CVE-2026-131190	7.5 HIGH
CVE-2026-131191	4.3 MEDIUM
CVE-2026-131192	7.5 HIGH
CVE-2026-131193	4.3 MEDIUM
CVE-2026-131194	4.6 MEDIUM
CVE-2026-131195	5.9 MEDIUM
CVE-2026-131196	7.5 HIGH

CVE	CVSS Score
CVE-2026-131197	6.4 MEDIUM
CVE-2026-76532	4.3 MEDIUM
CVE-2026-76533	4.2 MEDIUM
CVE-2026-76534	4.7 MEDIUM
CVE-2026-76535	9.1 CRITICAL
CVE-2026-76536	9.4 CRITICAL
CVE-2026-76537	4.3 MEDIUM
CVE-2026-76538	8.8 HIGH
CVE-2026-76539	6.5 MEDIUM
CVE-2026-76540	8.8 HIGH
CVE-2026-76541	4.8 MEDIUM
CVE-2026-76542	5.9 MEDIUM
CVE-2026-76543	5.4 MEDIUM
CVE-2026-76544	8.1 HIGH
CVE-2026-76545	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-116	Improper Encoding or Escaping of Output
CWE-117	Improper Output Neutralization for Logs
CWE-204	Observable Response Discrepancy
CWE-305	Authentication Bypass by Primary Weakness
CWE-352	Cross-Site Request Forgery
CWE-401	Missing Release of Memory after Effective Lifetime

CWE	Beschrijving
CWE-476	NULL Pointer Dereference
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-798	Use of Hard-coded Credentials
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

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.