



Advisory NCSC-2026-0412

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Splunk Enterprise

Publicatiedatum: 09-10-2026

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

De kwetsbaarheden betreffen verschillende versies van Splunk Enterprise en omvatten onder andere onvoldoende autorisatiecontroles in REST API endpoints, waardoor niet-bevoegde gebruikers toegang kunnen krijgen tot geprivilegieerde functionaliteit of gevoelige gegevens. Sommige kwetsbaarheden maken het mogelijk voor gebruikers zonder admin- of power-rollen om configuratiewijzigingen door te voeren, payloads te laten ondertekenen, of zoekopdrachten en loggegevens van andere gebruikers in te zien. Daarnaast zijn er problemen met onjuiste validatie van invoer, zoals SQL-injectie in SPL2 modules, manipulatie van indexnamen, en het injecteren van vervalste loggegevens. Verder is er een privilege-escalatie mogelijk tijdens pakketupgrades op Linux-systemen door vertrouwen op gemanipuleerde installatie-inhoud. Ook kunnen gebruikers met bepaalde rechten de broncode van de Discover Splunk Observability Cloud app inzien door blootstelling van embedded source maps. Andere kwetsbaarheden betreffen het omzeilen van toegangsrestricties tot interne indexen, het wijzigen van alertdata en mobiele ontvangerinformatie in key-value stores, en het creëren van gebruikersnamen met een punt aan het einde, wat leidt tot gedeelde configuratiegegevens. De kwetsbaarheden zijn aanwezig in meerdere recente versies van Splunk Enterprise en sommige ook in Splunk Secure Gateway.

Oplossingen

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

Referenties

- <https://advisory.splunk.com/advisories/SVD-2026-1001>
- <https://advisory.splunk.com/advisories/SVD-2026-1002>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76264	4.3 MEDIUM
CVE-2026-76265	6.5 MEDIUM
CVE-2026-76266	7.7 HIGH
CVE-2026-76267	4.3 MEDIUM
CVE-2026-76268	9.8 CRITICAL
CVE-2026-76269	6.5 MEDIUM
CVE-2026-76270	6.5 MEDIUM
CVE-2026-76271	6.5 MEDIUM
CVE-2026-76272	4.3 MEDIUM
CVE-2026-76273	4.3 MEDIUM
CVE-2026-76274	6.5 MEDIUM
CVE-2026-76275	4.3 MEDIUM
CVE-2026-76276	4.3 MEDIUM
CVE-2026-76277	4.1 MEDIUM
CVE-2026-76278	4.3 MEDIUM
CVE-2026-76279	4.3 MEDIUM
CVE-2026-76280	6.3 MEDIUM
CVE-2026-76281	5.3 MEDIUM
CVE-2026-76282	8.8 HIGH
CVE-2026-76283	7.6 HIGH
CVE-2026-76284	
CVE-2026-76285	

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-117	Improper Output Neutralization for Logs
CWE-306	Missing Authentication for Critical Function
CWE-407	Inefficient Algorithmic Complexity
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-1188	Initialization of a Resource with an Insecure Default

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.