Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0247

Kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2026

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 kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform.

Duiding

De eerste kwetsbaarheid betreft onvoldoende CSRF-bescherming en inputvalidatie in Deployment Server endpoints, waardoor een aanvaller willekeurige SPL-zoekopdrachten kan uitvoeren onder de splunk-system-user context met verhoogde privileges. Dit kan leiden tot ongeautoriseerde toegang tot gevoelige opgeslagen credentials en geïndexeerde data. De tweede kwetsbaarheid is een path traversal probleem waarbij gebruikers met bepaalde rollen apps kunnen installeren die bestanden buiten de bedoelde app-directory kunnen schrijven, specifiek in de $SPLUNK_HOME/etc/ directory en subdirectories. Dit kan resulteren in ongeautoriseerde wijziging van configuratiebestanden of andere gevoelige data. De derde kwetsbaarheid maakt het mogelijk voor gebruikers zonder 'admin' of 'power' rol om via het /servicesNS/-/-/storage/passwords REST endpoint en de |rest SPL-command toegang te krijgen tot opgeslagen credential hashes, doordat het veld encr_password wordt teruggegeven. Deze kwetsbaarheden beïnvloeden de integriteit en vertrouwelijkheid van data binnen de getroffen Splunk-producten.

Oplossingen

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

Referenties

- https://advisory.splunk.com/advisories/SVD-2026-0702
- https://advisory.splunk.com/advisories/SVD-2026-0703
- https://advisory.splunk.com/advisories/SVD-2026-0704

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20296	8.3 HIGH
CVE-2026-20297	7.2 HIGH
CVE-2026-20298	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-352	Cross-Site Request Forgery (CSRF)

Getroffen producten

Splunk
Splunk Cloud Platform
Splunk Enterprise

Disclaimer