Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0198

Kwetsbaarheden verholpen in Splunk Enterprise en Splunk Cloud Platform

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 15-06-2026

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 en Splunk Cloud Platform.

Duiding

De kwetsbaarheden betreffen verschillende onderdelen van Splunk Enterprise en Splunk Cloud Platform. Splunk heeft de kwetsbaarheid met kenmerk CVE-2026-20253 in de PostgreSQL sidecar service endpoint als kritiek beoordeeld en maakt het mogelijk voor niet-geauthenticeerde gebruikers om willekeurige bestanden aan te maken of te verwijderen door het ontbreken van authenticatiecontroles. Een andere kwetsbaarheid met kenmerk CVE-2026-20251 betreft een Remote Code Execution (RCE) via onveilige deserialisatie van KV Store data met de 'jsonpickle' Python library, waarbij laaggeprivilegieerde gebruikers zonder admin- of power-rollen code op afstand kunnen uitvoeren. Verder zijn meerdere kwetsbaarheden vastgesteld die het mogelijk maken om gevoelige gegevens te exfiltreren via onder meer SSRF-, CSS-injectie- en XSS-aanvallen. Door onvoldoende validatie van URL's, domeinen en gebruikersinvoer kunnen aanvallers beveiligingscontroles omzeilen, interne systemen benaderen en data buitmaken.

Oplossingen

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

Referenties

- https://advisory.splunk.com/advisories/SVD-2026-0601
- https://advisory.splunk.com/advisories/SVD-2026-0602
- https://advisory.splunk.com/advisories/SVD-2026-0603
- https://advisory.splunk.com/advisories/SVD-2026-0604
- https://advisory.splunk.com/advisories/SVD-2026-0605
- https://advisory.splunk.com/advisories/SVD-2026-0606
- https://advisory.splunk.com/advisories/SVD-2026-0607
- https://advisory.splunk.com/advisories/SVD-2026-0608
- https://advisory.splunk.com/advisories/SVD-2026-0609

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20253	9.8 CRITICAL

CVE-2026-20251	8.8 HIGH
CVE-2026-20252	7.6 HIGH
CVE-2026-20254	5.7 MEDIUM
CVE-2026-20255	5.7 MEDIUM
CVE-2026-20256	5.7 MEDIUM
CVE-2026-20257	5.7 MEDIUM
CVE-2026-20259	5.5 MEDIUM
CVE-2026-20258	7.1 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-284	Improper Access Control
CWE-306	Missing Authentication for Critical Function
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Splunk
Splunk Cloud Platform
Splunk Enterprise

Splunk Secure Gateway
splunk

Disclaimer