Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0513

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Splunk SOAR

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 heeft meerdere kwetsbaarheden verholpen in Splunk SOAR (versies eerder dan 8.8.0).

Duiding

De kwetsbaarheden in Splunk SOAR betreffen diverse componenten van het platform, waaronder de REST API, playbook API, container- en artifactbeheer, approval workflows, tenant- en labeltoegangscontrole, app- en dependency management, en audit logging.

Geauthenticeerde gebruikers met verschillende permissies kunnen door onvoldoende autorisatiecontroles en validaties onder meer ongeautoriseerde toegang verkrijgen tot gevoelige data, zoals container- en tenantinformatie, callback handles, approval prompts, en playbook runs buiten hun toegestane scope. Daarnaast kunnen zij acties uitvoeren zoals het manipuleren van container pins, het injecteren van malafide HTML/JavaScript in notes, het wijzigen van timestamps, en het creëren of importeren van containers en artifacts met onjuiste metadata of workflowstatussen. Sommige kwetsbaarheden maken het mogelijk om arbitrary code uit te voeren via onjuiste validatie van app dependencies, package references, of helper scripts binnen cluster lifecycle processen.

Verder zijn er problemen met het lekken van gevoelige credentials via onveilige API endpoints en inadequate logging van wijzigingen, wat de integriteit en vertrouwelijkheid van het systeem beïnvloedt. De kwetsbaarheden kunnen leiden tot privilege escalatie, ongeautoriseerde datatoegang, verstoring van geautomatiseerde processen, en mogelijke compromittering van het host-systeem.

De issues zijn specifiek voor Splunk SOAR versies onder 8.8.0 en betreffen onder andere de mechanismen voor toegangscontrole, contextbinding in playbook executies, en validatie van gebruikersinvoer binnen het platform.

Oplossingen

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

Referenties

- https://advisory.splunk.com/advisories/SVD-2026-1108

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-131240	3.5 LOW
CVE-2026-131241	4.3 MEDIUM
CVE-2026-131242	6.5 MEDIUM
CVE-2026-131243	7.6 HIGH
CVE-2026-131244	4.3 MEDIUM
CVE-2026-131245	7.1 HIGH
CVE-2026-131246	8.8 HIGH
CVE-2026-131247	4.3 MEDIUM
CVE-2026-131248	7.2 HIGH
CVE-2026-131249	4.3 MEDIUM
CVE-2026-131250	5.4 MEDIUM
CVE-2026-131251	4.3 MEDIUM
CVE-2026-131252	8.8 HIGH
CVE-2026-131253	9.9 CRITICAL
CVE-2026-131254	5.4 MEDIUM
CVE-2026-131255	7.5 HIGH
CVE-2026-131256	7.2 HIGH
CVE-2026-131257	5.4 MEDIUM
CVE-2026-131258	8.7 HIGH
CVE-2026-131259	5.4 MEDIUM
CVE-2026-131260	8.7 HIGH
CVE-2026-131261	8.8 HIGH
CVE-2026-131262	7.1 HIGH

CVE	CVSS Score
CVE-2026-131263	8.8 HIGH
CVE-2026-131264	6.3 MEDIUM
CVE-2026-131265	4.3 MEDIUM
CVE-2026-131266	7.7 HIGH
CVE-2026-131267	6.3 MEDIUM
CVE-2026-131268	7.2 HIGH
CVE-2026-131269	8.8 HIGH
CVE-2026-131270	8.8 HIGH
CVE-2026-131271	8.8 HIGH
CVE-2026-131272	7.2 HIGH
CVE-2026-131273	4.3 MEDIUM
CVE-2026-131274	2.7 LOW
CVE-2026-131275	5.4 MEDIUM
CVE-2026-131276	4.3 MEDIUM
CVE-2026-131277	6.3 MEDIUM
CVE-2026-131278	7.3 HIGH
CVE-2026-131279	4.3 MEDIUM
CVE-2026-131280	6.5 MEDIUM
CVE-2026-131281	4.3 MEDIUM
CVE-2026-131282	8.1 HIGH
CVE-2026-131283	4.3 MEDIUM
CVE-2026-131284	4.3 MEDIUM
CVE-2026-131285	6.5 MEDIUM
CVE-2026-131286	7.1 HIGH
CVE-2026-131287	9.6 CRITICAL
CVE-2026-131288	7.3 HIGH
CVE-2026-131289	3.1 LOW
CVE-2026-131290	4.3 MEDIUM
CVE-2026-131291	6.5 MEDIUM
CVE-2026-131292	6.5 MEDIUM
CVE-2026-131293	8.3 HIGH

CVE	CVSS Score
CVE-2026-131294	6.5 MEDIUM
CVE-2026-131295	8.8 HIGH
CVE-2026-131296	5.4 MEDIUM
CVE-2026-131297	8.1 HIGH
CVE-2026-131298	4.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-88	Improper Neutralization of Argument Delimiters in a Command
CWE-94	Improper Control of Generation of Code
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-214	Invocation of Process Using Visible Sensitive Information
CWE-427	Uncontrolled Search Path Element
CWE-522	Insufficiently Protected Credentials
CWE-532	Insertion of Sensitive Information into Log File
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-706	Use of Incorrectly-Resolved Name or Reference
CWE-778	Insufficient Logging
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes

Getroffen producten

Splunk
SOAR

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.