CYBER ADVISORY

TLP:CLEAR

29 March 2024

Splunk Vulnerabilities

CVE-2024-29945 | CVE-2024-29946 | Splunk | High Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of high vulnerabilities known as CVE-2024-29945 and CVE-2024-29946.[1] CVE-2024-29945 affects Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9. Exploitation may expose authentication tokens during the token validation process, which could occur when Splunk Enterprise is running in debug mode or when the JsonWebToken component is configured to log its activity at the DEBUG logging level.[2] CVE-2024-29946, affects Splunk Enterprise versions below 9.2.1, 9.1.4, and 9.0.9, as well as Splunk Cloud Platform versions below 9.1.2312.100. Exploitation may allow attackers to bypass SPL safeguards for risky commands with the permissions of a highly-privileged user in the Hub. The vulnerability would require the attacker to phish the victim by tricking them into initiating a request within their browser.[3]

The Cal-CSIC recommends upgrading to the appropriate patched version of Splunk when possible.

For further information applying Splunk patches, please refer to Splunk Customer Support.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Cyber Security News; "Multiple Splunk Vulnerabilities Attackers Bypass SPL Safeguards : Patch Now;" https://cybersecuritynews.com/splunk-vulnerabilities-spl-safeguards/; accessed 29 March 2024

[2] Splunk; "Splunk Authentication Token Exposure in Debug Log in Splunk Enterprise;" https://advisory.splunk.com/advisories/SVD-2024-0301; accessed 29 March 2024

[3] Splunk; "Risky command safeguards bypass in Dashboard Examples Hub;" https://advisory.splunk.com/advisories/SVD-2024-0302; accessed 29 March 2024