CYBER ADVISORY

Monday, June 22, 2026 **CAL-CSIC-202606-A-016**

Missing Authentication for Critical Function Vulnerability Affecting Splunk Enterprise

Authentication Flaw | Data Manipulation/Deletion | Proof-of-Concept Available | Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability impacting Splunk Enterprise. CVE-2026-20253 carries a CVSS 3.1 score of 9.8.[1] It is a critical authentication flaw in the PostgreSQL sidecar service endpoint of Splunk Enterprise. The vulnerability exists because the PostgreSQL sidecar service endpoint lacks authentication controls.

CVE-2026-20253 allows a remote, unauthenticated user to create or truncate any file on the system.[2] Successful exploitation would lead to complete system compromise, data manipulation/deletion, service disruption, and enabling pivots to other internal network resources.

Splunk has acknowledged this vulnerability and has published a security advisory. Their Product Security Incident Response Team (PSIRT) has noted that the vulnerability can be temporarily mitigated by disabling the PostgreSQL sidecar service. Additionally, their PSIRT is aware of limited exploitation of CVE-2026-20253.[3] Internal third-party sources are not aware of any zero-day exploitation. There is a publicly available Proof-of-Concept for this vulnerability.[4]

The Cal-CSIC recommends following Splunk's remediation and patching guidance as soon as possible. For additional details for CVE-2026-20253, please use this link:

Splunk Security Advisory: https://advisory.splunk.com/advisories/SVD-2026-0603

Affected Product and Version

Product	Affected Enterprise Version	Fixed Release Version
Splunk Enterprise	10.2.0 to 10.2.3	10.2.4
	10.0.0 to 10.0.6	10.0.7

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] OpenCVE; "CVE-2026-20253"; https://advisory.splunk.com/advisories/SVD-2026-0603; accessed 22 June 2026

[2] Picus; "Splunk CVE-2026-20253: Unauthenticated Remote Code Execution Vulnerability Explained"; https://www.picussecurity.com/resource/blog/splunk-cve-2026-20253-unauthenticated-remote-code-execution-vulnerability-explained; accessed 22 June 2026

[3] Splunk; "Unauthenticated Arbitrary File Creation and Truncation in a PostgreSQL Sidecar Service Endpoint in Splunk Enterprise"; https://advisory.splunk.com/advisories/SVD-2026-0603; accessed 22 June 2026

[4] Watchtowr Labs; "Why Use App-Level Auth When Every Database Has Auth? (Splunk Enterprise CVE-2026-20253 Pre-Auth RCE)"; https://labs.watchtowr.com/why-use-app-level-auth-when-every-database-has-auth-splunk-enterprise-cve-2026-20253-pre-auth-rce/; accessed 22 June 2026