CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
1 November 2024

Improper Authentication Vulnerability in Apache Solr

Solr Apache | Java | Bypass Security | PKIAuthentication

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-45216.[1] This vulnerability in Apache Solr has a maximum CVSS version 3.x score of 9.8, indicating severe risk[2] and is present in version 5.3.0 before 8.11.4 and version 9.0.0 before 9.7.0.[3] Solr Apache is an open-source enterprise-search platform, written in Java that is widely used for enterprise search and analytics use cases. CVE-2024-45216 allows for the authentication bypass of Solr instances using the PKIAuthenticationPlugin, which is enabled by default with Solr Authentication. By appending a fake ending at the end of any Solr API URL path, requests can bypass authentication while maintaining the API contract with the original URL Path. A proof of concept for this CVE is available[4].

The Cal-CSIC recommends immediately updating to the latest Solr Apache version.

For further information on applying updates please refer to Solr Apache Documentation.

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 here.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

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] National Vulnerability Database; “CVE-2024-45216 Detail” https://nvd.nist.gov/vuln/detail/CVE-2024-45216; accessed 1 November 2024

[2] ATTACKERKB; “CVE-2024-45216” https://attackerkb.com/topics/pKhCOpNnHj/cve-2024-45216; accessed 1 November 2024

[3] Solr Apache; “Solr Security News” https://solr.apache.org/security.html#cve-2024-45216-apache-solr-authentication-bypass-possible-using-a-fake-url-path-ending; accessed 1 November 2024

[4] Issues Apache; “Authentication bypass possible using a fake :/admin/info/key URL Path ending” https://issues.apache.org/jira/browse/SOLR-17417; accessed 1 November 2024

CAL-CSIC-202411-001

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

2