CYBER ADVISORY

TLP:CLEAR
15 October 2024

Keycloak Broken Access Control Vulnerability

CVE-2024-3656 | Keycloak | Proof of Concept | High

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high severity vulnerability known as CVE-2024-3656. The Keycloak vulnerability affects all versions up to 24.05.[1] A Proof of Concept demonstrates how any user can perform certain API actions reserved for Keycloak administrators.[2] Successful exploitation of the Keycloak vulnerability may lead to data breach or system compromise.[3]

The Cal-CSIC recommends immediately upgrading to Keycloak 26.

For further information on applying upgrades please refer to [Keycloak's upgrade 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 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] National Institute of Standards and Technology. (2024). *CVE-2024-3656*. NVD - Vulnerability Database. "https://nvd.nist.gov/vuln/detail/CVE-2024-3656"; Accessed 14 October 2024.

[2] GitHub. (2024). *CVE-2024-3656*. GitHub. "https://github.com/h4x0r-dz/CVE-2024-3656?tab=readme-ov-file"; Accessed 14 October 2024.

[3] Red Hat. (2024). *CVE-2024-3656*. Red Hat Customer Portal. "https://access.redhat.com/security/cve/CVE-2024-3656"; Accessed 14 October 2024.