CYBER ADVISORY

TLP:CLEAR

17 January 2024

Atlassian Confluence Vulnerability

CVE-2023-22527 | RCE | Confluence | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2023-22527.[1] The vulnerability affects Atlassian Confluence Data Center and Server 8 versions released before 5 December 2023, as well as 8.4.5.[2] The issue consists of a template injection vulnerability which could allow an unauthenticated attacker to achieve Remote Code Execution, (RCE) on an affected version.[3,4]

The Cal-CSIC recommends immediately upgrading to the appropriate patched version of the Confluence Data Center and Server.

For further information on applying upgrades, please refer to Atlassian Support CVE-2023-22527.

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.

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] Help Net Security; "Atlassian reveals critical Confluence RCE flaw, urges "immediate action" (CVE-2023-22527);" https://www.helpnetsecurity.com/2024/01/16/cve-2023-22527/; accessed 17 January 2024
[2] Github; "CVE-2023-22527 Confluence RCE;" https://github.com/Avento/CVE-2023-22527_Confluence_RCE; accessed 17 January 2024
[3] National Vulnerability Database; "CVE-2023-22527 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2023-22527; accessed 17 January 2024
[4] Dark Reading; "Patch ASAP: Max-Critical Atlassian Bug Allows Unauthenticated RCE;" https://www.darkreading.com/application-security/patch-max-critical-atlassian-bug-unauthenticated-rce; accessed 17 January 2024