National Cyber Security Centre

2401240199-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in Atlassian Confluence Data Center and Confluence Server (CVE-2023-22527)(CVSSv3: 9.8)

Thursday 25th January, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

Please treat this document in accordance with the TLP assigned.

Description

CVE Published: 2024-01-16T05:15:00
Vendor: Atlassian
Product: Confluence Data Center and Confluence Server
CVE ID: CVE-2023-22527
CVSS3.0 Score[1]**:** 9.8
EPSS Percentile[2]**:** 0.24036
Summary: A template injection vulnerability on older versions of Confluence Data Center and Server allows an unauthenticated attacker to achieve Remote Code Execution (RCE) on an affected instance. Customers using an affected version must take immediate action.

Most recent supported versions of Confluence Data Center and Server are not affected by this vulnerability as it was ultimately mitigated during regular version updates. However, Atlassian recommends that customers take care to install the latest version to protect their instances from non-critical vulnerabilities outlined in Atlassian's January Security Bulletin.

More information related to this issue can be found at the following link(s):
https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615

https://jira.atlassian.com/browse/CONFSERVER-93833

Products Affected

- Atlassian Confluence Data Center
- Confluence Server

Versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0-8.5.3.

Impact

CVE-2023-22527 is a template injection vulnerability that allows an unauthenticated attacker to achieve RCE on an affected version of Confluence Data Center and Confluence Server

Common Weakness Enumeration (CWE)[3]**:** RCE (Remote Code Execution) **Present in CISA Known Exploited Vulnerability(KEV)**[4] **catalog:** YES

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Atlassian.

Additional recommendations and mitigation's for CVE-2023-22527 can be found in the respective link(s) below:
https://confluence.atlassian.com/pages/viewpage.action?pageId=1333335615
https://jira.atlassian.com/browse/CONFSERVER-93833

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie