National Cyber Security Centre

2312060122-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical RCE Vulnerability In Confluence Data Center and Confluence Server - CVE-2023-22522

Wednesday 6th December, 2023

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

A critical Remote Code Execution (RCE) vulnerability, tracked as CVE-2023-22522 with a CVSS score of 9.0, has been discovered in Confluence Data Center and Server. This Template Injection vulnerability allows an authenticated attacker, including one with anonymous access, to inject unsafe user input into a Confluence page. Using this approach, an attacker is able to achieve RCE on an affected instance.

Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.

Products Affected

All versions including and after 4.0.0 of Confluence Data Center and Server:

- 4.x.x, 5.x.x, 6.x.x, 7.x.x
- 8.0.x, 8.1.x, 8.2.x, 8.3.x
- 8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4
- 8.5.0, 8.5.1, 8.5.2, 8.5.3

Confluence Data Center

- 8.6.0
- 8.6.1

Impact

Exploitation of CVE-2023-22522 could allow an attacker, even one with anonymous access, to inject hazardous user input into a Confluence page allowing the attacker to achieve Remote Code Execution (RCE) on any affected instance.

Recommendations

The NCSC strongly advises affected organisations to immediately patch your instance to a fixed version or a fixed LTS version as listed in the Atlassian security advisory.

If you are unable to patch to a fixed version, the following recommendations are advised:

- Back up your instance using Atlassians backup instructions
- Remove your instance from the internet and restrict external network access including those with user authentication until you can patch

Further information on this vulnerability from Atlassian can be found here:

- https://confluence.atlassian.com/security/cve-2023-22522-rce-vulnerability-in-confluence-data-center-and-confluence-server-1319570362.html
- https://confluence.atlassian.com/doc/production-backup-strategy-38797389.html

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