National Cyber Security Centre

2311090114-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical severity vulnerability in Atlassian Confluence Data Center and Server - CVE-2023-22518

Thursday 9th November, 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

Atlassian has discovered a critical severity vulnerability in its Confluence Data Center and Confluence Server products. The vulnerability is classified as an improper authorisation vulnerability meaning that that an attacker, even if unauthenticated, could exploit this weakness to gain unauthorised access or privileges within a Confluence system.

A proof of concept exploit is available. There are reports of active exploitation of this vulnerability resulting in data loss and/or encryption.

The issue is being tracked as CVE-2023-22518 with a CVSS score of 10: https://nvd.nist.gov/vuln/detail/CVE-2023-22518

Products Affected

All versions of Confluence Data Center and Server **prior** to the following versions:

- 7.19.16
- 8.3.4
- 8.4.4
- 8.5.3
- 8.6.1

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

Impact

Exploitation of CVE-2023-22518 could allow an attacker, even if unauthenticated, to reset a Confluence instance and create a Confluence instance administrator account. Using this account, an attacker could then perform all administrative actions that are available to a Confluence instance administrator leading to a full loss of confidentiality, integrity and availability.

There have been reports of the active exploitation of this vulnerability.

Recommendations

The NCSC strongly advises organisations to patch each of their affected instances to one of the listed fixed versions or any later version as listed in the Atlassian security advisory. Organisations should also

check all affected Confluence instances for evidence of compromise using Atlassian's threat detection advice contained in their advisory.

If organisations are unable to patch they are advised to apply the following temporary mitigations:

- Back up your instance
- Remove your instance from the internet until you can patch

Further information can be found in Atlassian's security advisory here:

- https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.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@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie