National Cyber Security Centre

2310050173-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical severity vulnerability in Atlassian Confluence Data Center and Server - CVE-2023-22515

Thursday 5th October, 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 released a security advisory for CVE-2023-22515, a critical severity zero-day privilege escalation vulnerability in Confluence Data Center and Server. Atlassian reports active exploitation of this vulnerability to create Confluence administrator accounts and access Confluence instances. Industry reporting has indicated that there may also be a risk of remote code execution.

Products Affected

Confluence Data Center and Confluence Server

- 8.0.0 - 8.0.4
- 8.1.0 - 8.1.1
- 8.1.3 - 8.1.4
- 8.2.0 - 8.2.3
- 8.3.0 - 8.3.2
- 8.4.0 - 8.4.2
- 8.5.0 - 8.5.1

Versions prior to 8.0.0 are not affected by this vulnerability.

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

Impact

Successful exploitation of this vulnerability would allow an attacker to create Confluence administrator accounts and to access Confluence instances.

Recommendations

The NCSC recommends that affected organisations apply the updates provided by Atlassian as soon as possible.

This vulnerability is being actively exploited. Therefore, if it is not possible to apply the patches immediately, affected organisations should take the following steps as recommended by Atlassian:

- Restrict access to the Confluence server from external connections
- Known attack vectors for this vulnerability can be blocked by preventing access to the /setup/* endpoints on Confluence instances.

Affected organisations should also check their infrastructure for the indicators of compromise published by Atlassian within their advisory.

Full details are available here: https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

Atlassian have published a FAQ here: https://confluence.atlassian.com/kb/faq-for-cve-2023-22515-1295682188.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