NCSC
National Cyber Security Centre

2206031001-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical Vulnerability in Atlassian Confluence Server and Data Center (CVE-2022-26134)

UPDATE 1

2022-06-03

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, 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.*

Revision History

Revision	Date	Author(s)	Description
1.0	03 June 2022	CSIRT-IE	Initial Alert created regarding a critical vulnerability in Atlassian Confluence Data Center and Server
1.1	03 June 2022	CSIRT-IE	Updated information on fixed versions and updated mitigation steps

Description

Volexity has published details related to a critical vulnerability in Atlassian Confluence Data Center and Server that is being actively exploited by threat actors. Atlassian describes it as a critical severity unauthenticated remote code execution vulnerability in Confluence Data Center and Server. The details of the bug are not public to help mitigation and limit exploitation of the vulnerability.

The NCSC recommends that affected organisations review the Atlassian's advice and upgrade to the latest Long Term Support release or apply the mitigation steps as soon as possible.

Products Affected

- All supported versions of Confluence Server and Data Center are affected.
  - **Note**: Atlassian reports that Atlassian Cloud sites are protected. This means that if your Confluence site is accessed via an Atlassian.net domain, it is hosted by Atlassian and is not vulnerable.

Impact

Unauthenticated remote code execution - compromised systems, data loss.

Mitigations

If you are unable to upgrade Confluence immediately, then as a temporary workaround, you can find specific mitigation steps for Confluence versions 7.15.0 - 7.18.0 and versions 7.0.0 - 7.14.2 in the Atlassian Advisory.

Recommendations

Atlassian have released the following versions to fix the issue:

- versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 and 7.18.1

NCSC recommends that affected organisations upgrade to the latest Long Term Support release as soon as possible. For a full description of the latest version, see the Confluence Server and Data Center Release Notes. You can download the latest version from the download centre.

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