National Cyber Security Centre

2307240144-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple RCE Vulnerabilities in Atlassian products

Monday 24th July, 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 its security bulletin for July 2023 to address Remote Code Execution (RCE) vulnerabilities in Confluence Data Center and Server (CVE-2023-22505 and CVE-2023-22508) and Bamboo Data Center (CVE-2023-22506). These RCE vulnerabilities can be exploited to take control of an affected system.

The Atlassian Security Bulletin can be found here: https://confluence.atlassian.com/security/security-bulletin-july-18-2023-1251417643.html.

Products Affected

The following supported products are affected:

- Version 8.0.0 of Confluence Data Center and Server
- Version 7.4.0 of Confluence Data Center and Server
- Version 8.0.0 of Bamboo Data Center

Impact

CVE-2023-22505: This RCE vulnerability allows an authenticated attacker to execute arbitrary code which has a high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction.

CVE-2023-22508: This RCE vulnerability allows an authenticated attacker to execute arbitrary code which has a high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction.

CVE-2023-22506: This code injection and RCE vulnerability allows an authenticated attacker to modify the actions taken by a system call and execute arbitrary code which has a high impact to confidentiality, high impact to integrity, high impact to availability, and no user interaction.

Recommendations

The NCSC strongly advises affected organisations to review the latest Atlassian Security Bulletin and apply available patches immediately. Further information can be found here:

- https://confluence.atlassian.com/security/security-bulletin-july-18-2023-1251417643.html
- https://jira.atlassian.com/browse/CONFSERVER-88265
- https://jira.atlassian.com/browse/BAM-22400
- https://jira.atlassian.com/browse/CONFSERVER-88221

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