NCSC
National Cyber Security Centre

2312070129-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

SnakeYAML Library RCE vulnerability impacts multiple Atlassian products - CVE-2022-1471 - CVSSv3: 9.8

Thursday 7th 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

Published: 2022-12-01T11:15:00
Vendor: Atlassian Data Center and Server Products
Product: SnakeYAML
CVE Number: CVE-2022-1471
CVSS3.0 Score: 9.8
EPSS: 0.712090000

Summary: Multiple Atlassian Data Center and Server Products use the SnakeYAML library for Java, which is susceptible to a deserialization flaw that can lead to RCE (Remote Code Execution).

SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

Atlassian has recommended that you patch each of your affected product installations to the latest version or one of the listed fixed versions below.

More information related to this issue can be found at the following link(s):

- https://confluence.atlassian.com/security/cve-2022-1471-snakeyaml-library-rce-vulnerability-in-multiple-products-1296171009.html
- https://github.com/google/security-research/security/advisories/GHSA-mjmj-j48q-9wg2
- https://bitbucket.org/snakeyaml/snakeyaml/issues/561/cve-2022-1471-vulnerability-in#comment-64581479
- https://www.github.com/mbechler/marshalsec/blob/master/marshalsec.pdf?ra
- https://groups.google.com/g/kubernetes-security-announce/c/mwrakFaEdnc
- https://security.netapp.com/advisory/ntap-20230818-0015/
- http://packetstormsecurity.com/files/175095/PyTorch-Model-Server-Registration-Deserialization-Remote-Code-Execution.html
- http://www.openwall.com/lists/oss-security/2023/11/19/1

Products Affected

- Automation for Jira app (including Server Lite edition)
- Bitbucket Data Center
- Bitbucket Server
- Confluence Data Center
- Confluence Server
- Confluence Cloud Migration App

- Jira Core Data Center
- Jira Core Server
- Jira Service Management Data Center
- Jira Service Management Server
- Jira Software Data Center
- Jira Software Server

See https://confluence.atlassian.com/security/cve-2022-1471-snakeyaml-library-rce-vulnerability-in-multiple-products-1296171009.html for further information on products/version affected.

Impact

Common Weakness Enumeration (CWE)[1]: CWE-20 Improper Input Validation

Present in CISA Known Exploited Vulnerability(KEV) catalog[2]: NO

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates.

Atlassian has recommended that you patch each of your affected product installations to the latest version as can be found at this link:

https://confluence.atlassian.com/security/cve-2022-1471-snakeyaml-library-rce-vulnerability-in-multiple-products-1296171009.html

[1] https://cwe.mitre.org/

[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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