NCSC
National Cyber Security Centre

2312060122-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in Atlassian Assets Discovery

Wednesday 6th 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

Atlassian has released an update to their Assets Discovery (formally Insight Discovery) scanning tool that addresses the vulnerability CVE-2023-22523. This is a critical vulnerability with a CVSS score of 9.8, which allows for Remote Code Execution (RCE).

Assets Discovery is a standalone network tool which can be downloaded from the Atlassian Marketplace.

The official Atlassian advisory can be found here: https://confluence.atlassian.com/security/cve-2023-22523-rce-vulnerability-in-assets-discovery-1319248914.html

Products Affected

This vulnerability affects all Assets Discovery prior to 3.2.0-cloud / 6.2.0 data center and server

Affected components versions of Assets Discovery component of Jira Service Management Cloud:

- Insight Discovery 1.0 - 3.1.3
- Assets Discovery 3.1.4 - 3.1.7
- Assets Discovery 3.1.8-cloud - 3.1.11-cloud

Affected components of Jira Service Management Data Center and Server:

- Insight Discovery 1.0 - 3.1.7
- Assets Discovery 3.1.9 - 3.1.11
- Assets Discovery 6.0.0 - 6.1.14, 6.1.14-jira-dc-8

Impact

Exploitation of CVE-2023-22523 could allow an attacker to perform privileged RCE (Remote Code Execution) on machines with the Assets Discovery agent installed.

To date, there have been no reports of the active exploitation of these vulnerabilities.

Recommendations

The NCSC strongly advises affected organisations to identify any assets that are running the Assets Discovery component within their environments, and to update affected components in line with their upgrade procedures.

Further information and some steps that organisations can take can be found here:

- https://confluence.atlassian.com/security/cve-2023-22523-rce-vulnerability-in-assets-discovery-1319248914.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@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie