CERT-EU Security Advisory 2019-009

Confluence Server Critical Remote Code Execution Vulnerability

April 15, 2019 — v1.0

History:

- *15/04/2019 — v1.0 – Initial publication*

Summary

A server-side template injection vulnerability has been discovered in Confluence Server and Data Center, in the Widget Connector. An attacker able to exploit this issue could achieve *path traversal* and *remote code execution* on systems that run a vulnerable version of Confluence Server or Data Center [1].

Technical Details

The Widget Connector macro in affected version of Atlassian Confluence Server allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection [2].

Products Affected

Atlassian Confluence Server affected versions include:

- before version 6.6.12 (the fixed version for 6.6.x),
- from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x),
- from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x),
- from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x).

Recommendations

Atlassian recommends that you upgrade to the latest version (6.15.1). For a full description of the latest version of Confluence Server and Data Center, see the Release Notes [3]. You can download the latest version of Confluence from the Atlassian website [4].

The versions of Confluence Server that address the issues:

- Confluence Server and Data Center versions 6.15.1 can be be downloaded from [4].

- Confluence Server and Data Center versions 6.6.12, 6.12.3, 6.13.3 and 6.14.2 can be be downloaded from [5].

If upgrading is not possible, see relevant instructions [6].

References

[1] https://jira.atlassian.com/browse/CONFSERVER-57974

[2] https://nvd.nist.gov/vuln/detail/CVE-2019-3396#vulnCurrentDescriptionTitle

[3] https://confluence.atlassian.com/doc/confluence-6-15-release-notes-965554120.html

[4] https://www.atlassian.com/software/confluence/download

[5] https://www.atlassian.com/software/confluence/download-archives

[6] https://confluence.atlassian.com/doc/confluence-security-advisory-2019-03-20-966660264.html