10 years CERT-EU

Security Advisory 2024-054

Confluence Data Center and Server Remote Code Execution

June 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/06/2024 — v1.0 – Initial publication*

Summary

A critical remote code execution (RCE) vulnerability, CVE-2024-21683, has been discovered in Atlassian's Confluence Data Center and Server. This vulnerability allows authenticated attackers with privileges of adding new macro languages to execute arbitrary code.

Technical Details

The vulnerability arises from insufficient input validation in the "Add a new language" function within the Configure Code Macro section. An attacker can exploit this by uploading a malicious Java file, leading to arbitrary code execution on the server.

Affected Products

- Confluence Data Center: Versions prior to 8.9.1
- Confluence Server: Versions prior to 8.5.9 LTS and 7.19.22 LTS

Recommendations

Immediately upgrade to Confluence Data Center version 8.9.1 or later, Confluence Server version 8.5.9 LTS, or 7.19.22 LTS.

References

[1] https://blog.sonicwall.com/en-us/2024/05/confluence-data-center-and-server-remote-code-execution-vulnerability

[2] https://confluence.atlassian.com/security/security-bulletin-may-21-2024-1387867145.html