Security Advisory 2022-040

Critical Remote Code Execution Vulnerability in Confluence

June 7, 2022 — v1.4

TLP:WHITE

History:
- 03/06/2022 — v1.0 – Initial publication
- 03/06/2022 — v1.2 – Update information about WAF workaround
- 04/06/2022 — v1.3 – Update information about patched versions and active exploitation
- 07/06/2022 — v1.4 – Update information about public POC and mitigation

Summary

On June 2, 2020, Confluence released an advisory about a critical vulnerability, identified CVE-2022-26134 with a severity score of 10 out of 10, which could lead to unauthenticated Remote Code Execution if exploited [1].

There is active exploitation of this vulnerability leading to installation of webshells and crypto-miners. Moreover, a POC of the vulnerability exploitation is now publicly available [5].

Technical Details

CVE-2022-26134 is an Object-Graph Navigation Language (OGNL) injection vulnerability that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance [4]. Exploiting it, attackers would be able to execute remote commands on the server without being authenticated and take full control of the server, for instance by uploading webshells [2].

Affected Products

All versions of Confluence Server and Data Center prior to the fixed versions listed below are affected by this vulnerability. Fixed versions include:
- 7.4.17
- 7.13.7
- 7.14.3
- 7.15.2
- 7.16.4
- 7.17.4
- 7.18.1
Please note that Confluence instances hosted directly in Atlassian Cloud are not affected

**Recommendations**

CERT-EU strongly recommends installing the latest version of Confluence servers.

As active exploitation of this vulnerability has been observed, CERT-EU strongly recommends scanning Confluence servers for IOCs published by the Volexity researchers [3] and for any other suspicious behaviour.

**Mitigation**

Where it is not possible to upgrade Confluence, while it is recommended, Atlassian teams provide workarounds for Confluence versions 7.15.0 until 7.18.0, and for Confluence versions 7.0.0 until Confluence 7.14.2 [1].

Nevertheless, the mitigation does not cover other security flaws fixed in the update.

**References**


[2] https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/

