CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-041

Critical Vulnerability in Jira Products

July 23, 2021 — v1.0

TLP:WHITE

History:

- *23/07/2021 — v1.0 – Initial publication*

Summary

A critical vulnerability (CVE-2020-36239) in many versions of Jira Data Center and Jira Service Management Data Center products can lead to arbitrary code execution [1].

Technical Details

The vulnerability stems from a missing authentication check or, in other words, unrestricted access to Ehcache RMI ports.

Ehcache is a widely used open-source cache used by Java applications for enhancing performance and scability. RMI refers to a remote method invocation, a concept in Java similar to remote procedure calls (RPC) in OOP languages. RMI lets programmers invoke methods present in remote objects—such as those present within an application running on a shared network, right from their application as they would run a local method or procedure. All this is done without the programmer having to worry about implementing the underlying networking functionality, which is where RMI APIs come in handy.

In this context, multiple Jira products expose an Ehcache RMI network service on ports 40001 and potentially 40011. Remote attackers can connect to these ports without requiring any authentication, and execute arbitrary code of their choice in Jira via object deserialization.

Affected Products

- Jira Data Center
- Jira Core Data Center
- Jira Software Data Center, and
- Jira Service Management Data Center

For specific version please check [1].

Recommendations

Atlassian recommends that upgrade to the latest versions. It also recommended restricting access to the Ehcache RMI ports (see workarounds). You can download the latest versions of Jira Data Center and Jira Service Management Data Center from the download centre Jira Data Center [3] respectively Jira Service Management Data Center [4].

CERT-EU recommends updating the vulnerable systems as soon as possible.

Workaround

Restrict access to the Ehcache RMI ports to Jira Data Center, Jira Core Data Center, and Jira Software Data Center, and Jira Service Management Data Center to only cluster instances via the use of firewalls or similar technologies.

For detailed instructions please refer to [1].

References

[1] https://confluence.atlassian.com/adminjiraserver/jira-data-center-and-jira-service-management-data-center-security-advisory-2021-07-21-1063571388.html

[2] https://www.bleepingcomputer.com/news/security/atlassian-asks-customers-to-patch-critical-jira-vulnerability/

[3] https://www.atlassian.com/software/jira/update

[4] https://www.atlassian.com/software/jira/service-management/update