CERT-EU

Security Advisory 2022-029

Oracle Java SE RCE Vulnerability

April 26, 2022 — v1.1

TLP:WHITE

History:

- *21/04/2022 — v1.0 – Initial publication*
- *26/04/2022 — v1.1 – Update about released exploit PoC*

Summary

Oracle published a Critical Patch Update Advisory - April 2022 which is a collection of patches for multiple security vulnerabilities. This Critical Patch Update contains 520 new security patches across the product families [1].

One of the vulnerabilities is **CVE-2022-21449**. It is an exploitable vulnerability which allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Exploitation of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data.

On the 20th of April, a researcher has released a Proof-of-Concept code [3], which make potential attacks much more likely.

Technical Details

The CVE-2022-21449 vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the Internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs [1, 2].

CVSS 3.1 Base Score is 7.5 (Integrity impacts).

Products Affected

Supported versions that are affected are:

- Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2 and 18
- Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2

Recommendations

Apply the latest fixes from the Oracle Critical Patch Update Advisory - April 2022 [1]. Since the exploit code is publicaly available [3], CERT-EU strongly recommends patching as soon as possible.

Workarounds

It may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of a successful attack. Both approaches may break application functionality, so testing on non-production systems is recommended. Neither approach should be considered a long-term solution as neither corrects the underlying problem [1].

References

[1] https://www.oracle.com/security-alerts/cpuapr2022.html

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21449

[3] https://github.com/khalednassar/CVE-2022-21449-TLS-PoC