Hive Pro

THREAT ADVISORY

A similar vulnerability like Log4shell discovered in H2 database console

TA2022004

Threat Level RED

Publish Date – Jan 10, 2022

An unauthenticated remote code execution vulnerability similar to Log4shell has been discovered in H2 Database (a popular Java SQL database) console and has been assigned CVE-2021-42392. It is claimed to be similar to the log4shell vulnerability since they both share the same root cause i.e they both are based on the Java Naming and Directory Interface (JNDI).

This flaw allows attacker-controlled URLs to be passed unfiltered to the javax.naming.Context.lookup function via numerous code paths in the H2 database system and execute remote code. The H2 database has an embedded web-based console for the database management which runs by default at http://localhost:8082. This console allows an unauthenticated attacker to run remote code execution as it fails to validate the parameters such as 'User Name' and 'Password' before performing lookup with the malicious URL in 'JDBC URL' field.

Organizations using an H2 console which is exposed to LAN or WAN should update H2 database to version 2.0.206 immediately.

Upgrading to version 2.0.206 eliminates this vulnerability. However, organization who cannot upgrade to version 2.0.206 can use either of the mitigations below:

1. The newer version of Java contains **trustURLCodebase** that does not allow remote codebases to load via JNDI, so upgrading to the latest version of Java (JRE/JDK) will eliminate this vulnerability. However, this mitigation can be bypassed sending a serialized "gadget" Java object through LDAP.
2. When the H2 console Servlet is installed on a web server, a security constraint can be introduced to restrict access to the console page to specified users.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-42392	H2 database versions 1.1.100 to 2.0.204	cpe:2.3:a:h2database:h2:*:*:*:*:*:*:*:*	H2 Database code execution	CWE-20, CWE-94

Patch Links

https://github.com/h2database/h2database/releases/tag/version-2.0.206
https://www.h2database.com/html/main.html

References

https://jfrog.com/blog/the-jndi-strikes-back-unauthenticated-rce-in-h2-database-console/
https://github.com/h2database/h2database/security/advisories/GHSA-h376-j262-vhq6
https://github.com/cybersecurityworks553/CVE-2021-42392-Detect
https://exchange.xforce.ibmcloud.com/vulnerabilities/216834