Hive Pro

# THREAT ADVISORY

## Apache Cassandra database affected by easily exploitable Remote code execution

**TA2022037**

**Threat Level** AMBER

**Publish Date –** Feb 18, 2022

Apache Cassandra is a database software being used by many companies such as Uber, Facebook, Netflix, Twitter, Instagram, Spotify, Instacart, Reddit, and Accenture. A remote code execution flaw (CVE-2021-44521) is reported which is easily exploitable and has the potential to wreak havoc on systems.

This vulnerability affects the Apache Cassandra instances that have the following non-default configuration settings:

enable_user_defined_functions: true
enable_scripted_user_defined_functions: true
enable_user_defined_functions_threads: false

An attacker with sufficient permissions to construct user defined functions in the cluster might use these setups to execute arbitrary code on the host system.

This vulnerability could be easily mitigated by either
setting 'enable_user_defined_functions_threads: true', or
upgrading versions 3.0.x to 3.0.26, 3.11.x to 3.11.12 or 4.0.x to 4.0.2

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
TA0002: Execution
T1190: Exploit-public facing application
T1059: Command and Scripting Interpreter
T1059.007: Command and Scripting Interpreter: JavaScript

## Vulnerability Details

| CVE ID | Affected Products | Affected CPE | Vulnerability Name | CWE ID |
|---|---|---|---|---|
| CVE-2021-44521 | Apache Cassandra 3.0 up to 3.0.26, 3.11 up to 3.11.12, 4.0 up to 4.0.2 | cpe:2.3:a:apache:cassandra:*:*:*:*:*:*:*:* | Remote code execution for scripted UDFs | CWE-94 |

## Patch Link

https://www.apache.org/dyn/closer.lua/cassandra/4.0.3/apache-cassandra-4.0.3-bin.tar.gz
https://www.apache.org/dyn/closer.lua/cassandra/3.11.12/apache-cassandra-3.11.12-bin.tar.gz
https://www.apache.org/dyn/closer.lua/cassandra/3.0.26/apache-cassandra-3.0.26-bin.tar.gz

### References

https://lists.apache.org/thread/y4nb9s4co34j8hdfmrshyl09lokm7356
https://jfrog.com/blog/cve-2021-44521-exploiting-apache-cassandra-user-defined-functions-for-remote-code-execution/