Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Shell Command Injection Vulnerability found in Apache Spark

Date of Publication

July 27, 2022

Admiralty code

A2

TA Number

TA2022158

Summary

Apache Spark recently disclosed a weakness, CVE-2022-33891, which would allow threat actors to execute arbitrary shell commands as a Spark user

CVE Table

CVE	NAME	PATCH
CVE-2022-33891	OS command injection	✓

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1202** Indirect Command Execution	**TA0002** Execution	**T1059** Command and Scripting Interpreter
TA0001 Initial Access	**T1190** Exploit Public-Facing Application		

Technical Details

The Spark UI's ability to enable Active Control Lists (ACLs) via the sparks.acls.enable option is the source of this security flaw. If ACLs are enabled, a HttpSecurityFilter code path allows impersonation by serving an arbitrary user name. In the event of success, an attacker can use a permission check function to launch a Unix shell command. It will result in the execution of arbitrary shell commands.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-33891	Apache Spark Versions 3.0.3 and earlier, 3.1.1 to 3.1.2, and 3.2.0 to 3.2.1.	cpe:2.3:a:apache_foundation:apache_spark:3.2.1:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.2.0:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.0.3:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.1.2:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.1.1:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.0.2:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.0.1:*:*:*:*:*:*:* cpe:2.3:a:apache_foundation:apache_spark:3.0.0:*:*:*:*:*:*:*	CWE-78

Patch Links

https://spark.apache.org/downloads.html

References

https://lists.apache.org/thread/p847l3kopoo5bjtmxrcwk21xp6tjxqlc

https://github.com/HuskyHacks/cve-2022-33891/blob/main/README.md

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization’s attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 27, 2022 • 6:42 AM

More at www.hivepro.com