Security Advisory 2022-058

Critical Shell Command Injection Vulnerability in Apache Spark

August 3, 2022 — v1.0

TLP:WHITE

History:

- *03/08/2022 — v1.0 – Initial publication*

Summary

On July 18, Apache Spark released a security bulletin [1] regarding a newly found critical vulnerability within Apache Spark's ACL implementation, tracked as **CVE-2022-33891** and with a CVSS score of 8.8 out of 10. The flaw was discovered by a security researcher, with the proof of concept (PoC) exploit already available on GitHub [2] and exploitation attempts in the wild being detected since, at least, July 26th.

Apache Spark is an open-source, unified engine for large-scale data analytics, which executes data engineering, data science, and machine learning tasks. Additionally, it provides high-level APIs in multiple programming languages[3].

Technical Details

The flaw could allow adversaries to perform **arbitrary shell command execution** as a current Spark user. The issue stems from the Apache Spark UI ability to enable ACLs via the configuration option `spark.acls.enable`.

If ACLs are enabled, a HttpSecurityFilter code path allows adversaries to perform impersonation by providing an arbitrary user name. In case of success, an attacker will be able to reach a permission check function, which will allow them to launch a Unix shell command. This eventually leads to the arbitrary shell command execution.

Affected Products

The following Apache Spark versions are affected by this flaw:

- 3.0.3 and earlier
- 3.1.1 to 3.1.2
- 3.2.0 to 3.2.1

Recommendations

To ensure your instances are protected from exploitation attempts, it is highly recommended to upgrade to Apache Spark maintenance release:

- 3.1.3
- 3.2.2
- 3.3.0 or later

References

[1] https://lists.apache.org/thread/p847l3kopoo5bjtmxrcwk21xp6tjxqlc

[2] https://github.com/W01fh4cker/cve-2022-33891

[3] https://spark.apache.org/