

CVE-2022-33891

Apache Spark Command Injection Vulnerability

CISA KEV since Mar 7, 2023

Actively exploited

Public exploit module (Metasploit)

The Apache Spark UI offers the possibility to enable ACLs via the configuration option `spark.acls.enable`. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in `HttpSecurityFilter` can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it.

EVRS 84/100 Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.932 99.84th percentile · FIRST	CISA DEADLINE Mar 28, 2023 KEV since 2023 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.932 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

This will result in arbitrary shell command execution as the user Spark is currently running as. This affects Apache Spark versions 3.0.3 and earlier, versions 3.1.1 to 3.1.2, and versions 3.2.0 to 3.2.1.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
spark	$\leq 3.0.3$ $\geq 3.1.1 \leq 3.1.2$ $\geq 3.2.0 \leq 3.2.1$	after 3.0.3 · after 3.1.2 · after 3.2.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4x9r-j582-cgr8

lists.apache.org lists.apache.org/thread/p847l3kopoo5bjtmxrcwk21xp6tjxqlc

NVD nvd.nist.gov/vuln/detail/CVE-2022-33891

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-0217

Current data evulnable.com/vulnerability-management/cve/CVE-2022-33891

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.