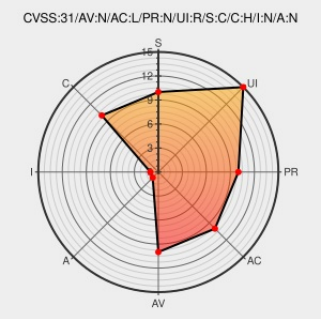
CVE-2020-15087

Published on: 06/30/2020 12:00:00 AM UTC

Last Modified on: 10/21/2022 06:01:00 PM UTC

CVE-2020-15087 - advisory for GHSA-f6pc-crhh-cp96

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Presto from Prestosql contain the following vulnerability:

In Presto before version 337, authenticated users can bypass authorization checks by directly accessing internal APIs. This impacts Presto server installations with secure internal communication configured. This does not affect installations that have not configured secure internal communication, as these installations are inherently insecure. This only affects Presto server installations. This does NOT affect clients such as the CLI or JDBC driver. This vulnerability has been fixed in version 337. Additionally, this issue can be mitigated by blocking network access to internal APIs on the coordinator and workers.

CVE-2020-15087 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **prestosql** - **Presto** version **< 337**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Release 337 (25 Jun 2020) — Trino 351 Documentation	trino.io text/html	MISC trino.io/docs/current/release/release-337.html#security-changes
Privilege escalation for internal APIs · Advisory · prestosql/presto · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/prestosql/presto/security/advisories/GHSA-f6pc-crhh-cp96
Release 337 (25 Jun 2020) — Presto 348 Documentation	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC prestosql.io/docs/current/release/release-337.html#security-changes

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

982807 Java (maven) Security Update for io.prestosql:presto-server (GHSA-f6pc-crhh-cp96)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Prestosql	Presto	All	All	All	All
Application	Prestosql	Presto	All	All	All	All

cpe:2.3:a:prestosql:presto:*:*:*:*:*:*:*:*:

cpe:2.3:a:prestosql:presto:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report