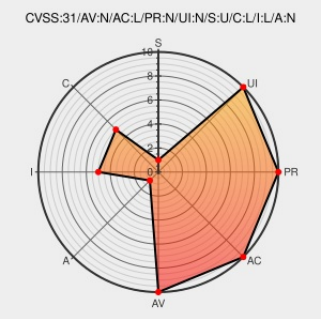
CVE-2021-39228

Published on: 09/17/2021 12:00:00 AM UTC

Last Modified on: 09/30/2021 07:02:00 PM UTC

CVE-2021-39228 - advisory for GHSA-mc22-5q92-8v85

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



Certain versions of Tremor from Linuxfoundation contain the following vulnerability:

Tremor is an event processing system for unstructured data. A vulnerability exists between versions 0.7.2 and 0.11.6. This vulnerability is a memory safety Issue when using `patch` or `merge` on `state` and assign the result back to `state`. In this case, affected versions of Tremor and the tremor-script crate maintains references to memory that might have been freed already. And these memory regions can be accessed by retrieving the `state`, e.g. send it over TCP or HTTP. This requires the Tremor server (or any other program using tremor-script) to execute a tremor-script script that uses the mentioned language construct. The issue has been patched in version 0.11.6 by removing the optimization and always cloning the target expression of a Merge or Patch. If an upgrade is not possible, a possible workaround is to avoid the optimization by introducing a temporary variable and not immediately reassigning to `state`.

CVE-2021-39228 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **tremor-rs** - **tremor-runtime** version **> 0.7.2, < 0.11.6**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Remove patch and merge in_place optimizations. · tremor-rs/tremor-runtime@1a2efcd · GitHub	github.com text/html	MISC github.com/tremor-rs/tremor-runtime/commit/1a2efcdbe68e5e7fd0a05836ac32d2cde78a0b2e
Release v0.11.6 - Fix Memory safety issue · tremor-rs/tremor-runtime · GitHub	github.com text/html	MISC github.com/tremor-rs/tremor-runtime/releases/tag/v0.11.6
Remove in-place optimizations of patch and merge by mfelsche · Pull Request #1217 · tremor-rs/tremor-runtime · GitHub	github.com text/html	MISC github.com/tremor-rs/tremor-runtime/pull/1217
Memory Safety Issue when using patch or merge on state and assign the result back to state · Advisory · tremor-rs/tremor-runtime · GitHub	github.com text/html	CONFIRM github.com/tremor-rs/tremor-runtime/security/advisories/GHSA-mc22-5q92-8v85

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Tremor	All	All	All	All

cpe:2.3:a:linuxfoundation:tremor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39228 : Tremor is an event processing system for unstructured data. A vulnerability exists between version… twitter.com/i/web/status/1…	2021-09-17 14:08:52
@threatmeter	CVE-2021-39228 Tremor is an event processing system for unstructured data. A vulnerability exists between versions… twitter.com/i/web/status/1…	2021-09-18 07:09:41

← Previous ID

Next ID→

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