GitHub Advisory Database / Unreviewed / CVE-2019-11922

A race condition in the one-pass compression functions of...

High severity Unreviewed Published on May 24, 2022 to the GitHub Advisory Database • Updated on Apr 4, 2024

Package

No package listed— Suggest a package

Affected versions

Unknown

Patched versions

Unknown

Description

A race condition in the one-pass compression functions of Zstandard prior to version 1.3.8 could allow an attacker to write bytes out of bounds if an output buffer smaller than the recommended size was used.

References

- https://nvd.nist.gov/vuln/detail/CVE-2019-11922
- facebook/zstd@`3e5cdf1`
- https://www.facebook.com/security/advisories/cve-2019-11922
- https://www.oracle.com/security-alerts/cpuoct2020.html
- http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00008.html
- http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00062.html
- http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00078.html
- https://usn.ubuntu.com/4108-1

Published by the National Vulnerability Database on Jul 25, 2019

Published to the GitHub Advisory Database on May 24, 2022

Last updated on Apr 4, 2024

Severity

High 8.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS score

0.634% (70th percentile)

Weaknesses

▶ CWE-362

CVE ID

CVE-2019-11922

GHSA ID

GHSA-w77f-wv46-4vcx

Source code

No known source code

Dependabot alerts are not supported on this advisory because it does not have a package from a supported ecosystem with an affected and fixed version.

Learn more about GitHub language support

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.