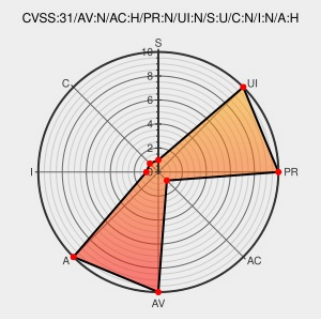
CVE-2023-28638

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:10:00 AM UTC

CVE-2023-28638 - advisory for GHSA-838x-pcvx-6p5w

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



Certain versions of Snappier from Snappier Project contain the following vulnerability:

Snappier is a high performance C# implementation of the Snappy compression algorithm. This is a buffer overrun vulnerability that can affect any user of Snappier 1.1.0. In this release, much of the code was rewritten to use byte references rather than pointers to pinned buffers. This change generally improves performance and reduces workload on the garbage collector. However, when the garbage collector performs compaction and rearranges memory, it must update any byte references on the stack to refer to the updated location. The .NET garbage collector can only update these byte references if they still point within the buffer or to a point one byte past the end of the buffer. If they point outside this area, the buffer itself may be moved while the byte reference stays the same. There are several places in 1.1.0 where byte references very briefly point outside the valid areas of buffers. These are at locations in the code being used for buffer range checks. While the invalid references are never dereferenced directly, if a GC compaction were to occur during the brief window when they are on the stack then it could invalidate the buffer range check and allow other operations to overrun the buffer. This should be very difficult for an attacker to trigger intentionally. It would require a repetitive bulk attack with the hope that a GC compaction would occur at precisely the right moment during one of the requests. However, one of the range checks with this problem is a check based on input data in the decompression buffer, meaning malformed input data could be used to increase the chance of success. Note that any resulting buffer overrun is likely to cause access to protected memory, which will then cause an exception and the process to be terminated. Therefore, the most likely result of an attack is a denial of service. This issue has been patched in release 1.1.1. Users are advised to upgrade. Users unable to upgrade may pin buffers to a fixed location before using them for compression or decompression to mitigate some, but not all, of these cases. At least one temporary decompression buffer is internal to the library and never pinned.

CVE-2023-28638 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **brantburnett** - **Snappier** version **= = 1.1.0**

CVSS3 Score: 5.9 - MEDIUM

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

CVE References

Description	Tags	Link
Short-lived stack references to locations outside buffers may become invalid if they exist during a GC compaction · Advisory · brantburnett/Snappier · GitHub	github.com text/html	MISC github.com/brantburnett/Snappier/security/advisories/GHSA-838x-pcvx-6p5w
Allow ref byte to point just past the end of spans (#73) · brantburnett/Snappier@d7ac526 · GitHub	github.com text/html	MISC github.com/brantburnett/Snappier/commit/d7ac5267b5b18439e6d108f8138edf48c436b32f

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snappier Project	Snappier	1.1.0	All	All	All

cpe:2.3:a:snappier_project:snappier:1.1.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28638 : Snappier is a high performance C# implementation of the Snappy compression algorithm. This is a bu… twitter.com/i/web/status/1…	2023-03-27 21:16:35
/r/netcve	CVE-2023-28638	2023-03-27 22:38:54

← Previous ID

Next ID→

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