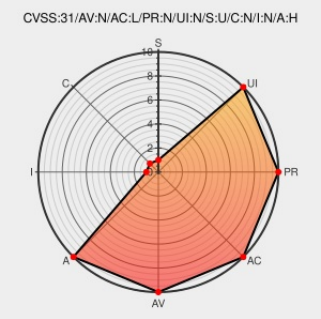
CVE-2018-1000052

Published on: 02/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1000052

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



Certain versions of Fmt from Fmt contain the following vulnerability:

fmtlib version prior to version 4.1.0 (before commit 0555cea5fc0bf890afe0071a558e44625a34ba85) contains a Memory corruption (SIGSEGV), CWE-134 vulnerability in fmt::print() library function that can result in Denial of Service. This attack appear to be exploitable via Specifying an invalid format specifier in the fmt::print() function results in a SIGSEGV (memory corruption, invalid write). This vulnerability appears to have been fixed in after commit 8cf30aa2be256eba07bb1cefb998c52326e846e7.

CVE-2018-1000052 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix segfault on complex pointer	Patch	CONFIRM

Fix segfault on complex pointer formatting (#642) · fmtlib/fmt@8cf30aa · GitHub	Patch github.com text/html	CONFIRM github.com/fmtlib/fmt/commit/8cf30aa2be256eba07bb1cefb998c52326e846e7
Segmentation fault in fmt::print() (memory corruption, invalid write of size 1) · Issue #642 · fmtlib/fmt · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	CONFIRM github.com/fmtlib/fmt/issues/642

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fmt	Fmt	All	All	All	All
Application	Fmt	Fmt	All	All	All	All

cpe:2.3:a:fmt:fmt:*:*:*:*:*:*:*:*:

cpe:2.3:a:fmt:fmt:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→