



CVE-2018-1000052

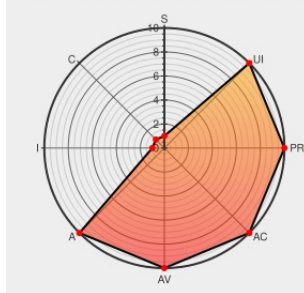
Published on: 02/09/2018 12:00:00 AM UTC

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

CVE-2018-1000052

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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 [M](#) [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
Fixes a buffer overflow in complex printer	Print	CONFIRM

CONFIRM

github.com/fmtlib/fmt/commit/8cf30aa2be256eba07bb1cefb998c52326e846e7

- Exploit
- Issue Tracking
- Third Party Advisory
- github.com
- text/html



comment@cve.report.

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→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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