



CVE-2018-17942

Published on: 10/03/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:54:00 AM UTC

CVE-2018-17942

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

Certain versions of [Gnulib](#) from [Gnu](#) contain the following vulnerability:

The `convert_to_decimal` function in `vasnprintf.c` in Gnulib before 2018-09-23 has a heap-based buffer overflow because memory is not allocated for a trailing `\0` character during `%f` processing.

CVE-2018-17942 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 30 Update: gnulib-0-31.20200107git.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-acac61cfd0

vasnprintf: Fix heap memory
overrun bug. ·
coreutils/gnulib@278b417 ·
GitHub

Patch
Third Party Advisory
github.com
text/html

MISC
github.com/coreutils/gnulib/commit/278b4175c9d7dd47c1a3071554aac02add3b3c35

PSPP - Bugs: bug #54686,
heap-buffer-overflow in csv
driver... [Savannah]

Exploit
Vendor Advisory
savannah.gnu.org
text/html

MISC savannah.gnu.org/bugs/?func=detailitem&item_id=54686

write past end of buffer in
vasnprintf() implementation
of %f

Exploit
Mailing List
Vendor Advisory
lists.gnu.org
text/x-diff

MISC lists.gnu.org/archive/html/bug-gnulib/2018-09/msg00107.html

[SECURITY] Fedora 31
Update: gnulib-0-
31.20200107git.fc31 -
package-announce - Fedora
Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2020-663f619e9c

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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	Gnu	Gnulib	All	All	All	All
Application	Gnu	Gnulib	All	All	All	All
cpe:2.3:a:gnu:gnulib:*****:						
cpe:2.3:a:gnu:gnulib:*****:						

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve/).

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