

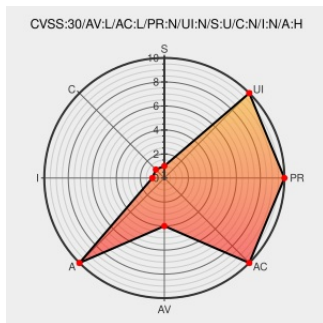


CVE-2011-5320

Published on: 10/18/2017 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:09:00 AM UTC

CVE-2011-5320

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

Certain versions of [Glibc](#) from [Gnu](#) contain the following vulnerability: `scanf` and related functions in `glibc` before 2.15 allow local users to cause a denial of service (segmentation fault) via a large string of 0s.

CVE-2011-5320 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.2 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
sourceware.org Git - glibc.git/commitdiff	sourceware.org text/xml	CONFIRM sourceware.org/git/?p=glibc.git;a=commitdiff;h=3f8cc204fdd0
sourceware.org Git - glibc.git/commitdiff	sourceware.org text/xml	CONFIRM sourceware.org/git/?p=glibc.git;a=commitdiff;h=20b38e0

Bug 13138 – scanf crashes on very long numbers	Issue Tracking sourceware.org text/html	 CONFIRM sourceware.org/bugzilla/show_bug.cgi?id=13138#c4
oss-security - Re: CVE request: glibc scanf implementation crashes on certain inputs	Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20150312 Re: CVE request: glibc scanf implementation crashes on certain inputs
'[Gimp-developer] scanf without field width limits making Gimp crash' - MARC	Exploit marc.info text/x-c	 MISC marc.info/?l=gimp-developer&m=129567990905823&w=2
1196745 – (CVE-2011-5320) CVE-2011-5320 glibc: scanf implementation crashes on certain inputs	Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1196745

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	Glibc	All	All	All	All
<code>cpe:2.3:a:gnu:glibc:*:*:*:*:*</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)