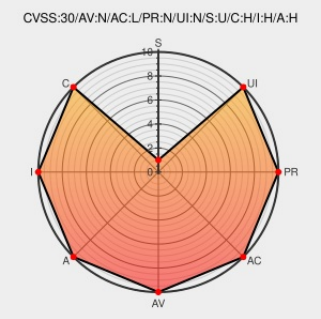
CVE-2018-6551

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

Last Modified on: 03/23/2021 11:24:47 PM UTC

CVE-2018-6551

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



Certain versions of Glibc from Gnu contain the following vulnerability:

The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.

CVE-2018-6551 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
22774 – (CVE-2018-6551) Integer overflow in _int_malloc (CVE-2018-6551)	Issue Tracking, Mailing List, Third Party Advisory, sourceware.org, text/html	CONFIRM sourceware.org/bugzilla/show_bug.cgi?id=22774

sourceware.org Git - glibc.git/commit	Issue Tracking Patch sourceware.org text/xml	CONFIRM sourceware.org/git/?p=glibc.git;a=commit;h=8e448310d74b283c5cd02b9ed7fb997b47bf9b22
February 2018 GNU C Library Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20190404-0003/

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

cpe:2.3:a:gnu:glibc:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→