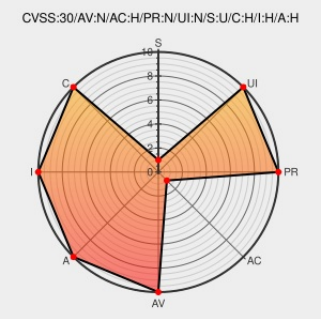
CVE-2017-17426

Published on: 12/05/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:27 PM UTC

CVE-2017-17426

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



Certain versions of Glibc from Gnu contain the following vulnerability:

The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check.

CVE-2017-17426 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
sourceware.org Git - glibc.git/commit	Patch, sourceware.org, text/xml	CONFIRM sourceware.org/git/gitweb.cgi?p=glibc.git;h=34697694e8a93b325b18f25f7dcded55d6baeaf6

22375 – (CVE-2017-17426) malloc returns pointer from tcache_get when should return NULL (CVE-2017-17426)	Exploit Issue Tracking sourceware.org text/html	CONFIRM sourceware.org/bugzilla/show_bug.cgi?id=22375

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	2.26	All	All	All
Application	Gnu	Glibc	2.26	All	All	All

cpe:2.3:a:gnu:glibc:2.26:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:glibc:2.26:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→