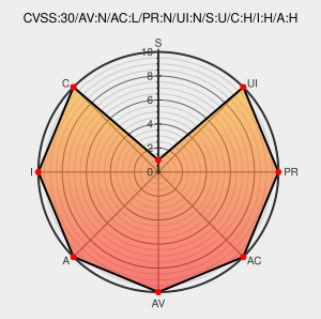
CVE-2017-18269

Published on: 05/18/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18269

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



Certain versions of Glibc from Gnu contain the following vulnerability:

An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686/multiarch/memcpy-sse2-unaligned.S in the GNU C Library (aka glibc or libc6) 2.21 through 2.27 does not correctly perform the overlapping memory check if the source memory range spans the middle of the address space, resulting in corrupt data being produced by the copy operation. This may disclose information to context-dependent attackers, or result in a denial of service, or, possibly, code execution.

CVE-2017-18269 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
22644 – (CVE-2017-18269) memmove-sse2-unaligned on 32bit x86 produces garbage	Issue Tracking sourceware.org	MISC sourceware.org/bugzilla/show_bug.cgi?id=22644

when crossing 2GB threshold (CVE-2017-18269)	text/html	
GitHub - fingolfin/memmove-bug: Reproducing a bug in GNU libc's memmove	Third Party Advisory github.com text/html	MISC github.com/fingolfin/memmove-bug
sourceware.org Git - glibc.git/commit	Patch sourceware.org text/xml	MISC sourceware.org/git/gitweb.cgi?p=glibc.git;h=cd66c0e584c6d692bc8347b5e72723d02b8a8ada
May 2018 GNU C Library Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20190401-0001/
NetApp Product Security	security.netapp.com text/html Inactive Link Not Archived	CONFIRM security.netapp.com/advisory/ntap-20190329-0001/
USN-4416-1: GNU C Library vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4416-1

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
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

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

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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