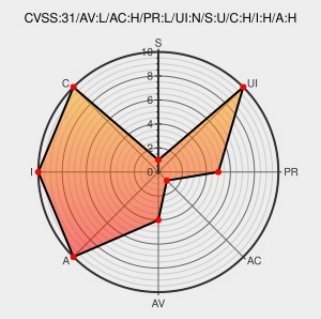
CVE-2017-1000376

Published on: 06/19/2017 12:00:00 AM UTC

Last Modified on: 09/22/2023 06:25:00 PM UTC

CVE-2017-1000376

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

libffi requests an executable stack allowing attackers to more easily trigger arbitrary code execution by overwriting the stack. Please note that libffi is used by a number of other libraries. It was previously stated that this affects libffi version 3.2.1 but this appears to be incorrect. libffi prior to version 3.1 on 32 bit x86 systems was vulnerable, and upstream is believed to have fixed this issue in version 3.1.

CVE-2017-1000376 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory access.redhat.com	CONFIRM access.redhat.com/security/cve/CVE-2017-1000376

	text/html	
Oracle Critical Patch Update Advisory - January 2020	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujan2020.html
	Mailing List Third Party Advisory www.qualys.com text/plain	MISC www.qualys.com/2017/06/19/stack-clash/stack-clash.txt
Debian -- Security Information -- DSA-3889-1 libffi	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3889

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libffi Project	Libffi	All	All	All	All
Application	Oracle	Peopletools	8.56	All	All	All
Application	Oracle	Peopletools	8.57	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Enterprise Virtualization Server	-	All	All	All
Application	Redhat	Enterprise Virtualization Server	-	All	All	All
Application	Redhat	Openshift	2.0	All	All	All
Application	Redhat	Openshift	2.0	All	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

cpe:2.3:a:libffi_project:libffi:*:*:*:*:*:*:*:*

cpe:2.3:a:oracle:peopletools:8.56:*:*:*:*:*:*:*

cpe:2.3:a:oracle:peopletools:8.57:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:enterprise_virtualization_server:-:*:*:*:*:*:*:*

cpe:2.3:a:redhat:enterprise_virtualization_server:-:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openshift:2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openshift:2.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→