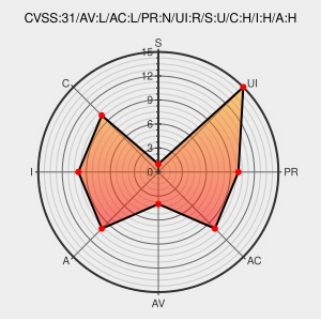
CVE-2019-18397

Published on: 11/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:06 PM UTC

CVE-2019-18397

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



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

A buffer overflow in the fribidi_get_par_embedding_levels_ex() function in lib/fribidi-bidi.c of GNU FriBidi through 1.0.7 allows an attacker to cause a denial of service or possibly execute arbitrary code by delivering crafted text content to a user, when this content is then rendered by an application that uses FriBidi for text layout calculations. Examples include any GNOME or GTK+ based application that uses Pango for text layout, as this internally uses FriBidi for bidirectional text layout. For example, the attacker can construct a crafted text file to be opened in GEdit, or a crafted IRC message to be viewed in HexChat.

CVE-2019-18397 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
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

[SECURITY] Fedora 31 Update: fribidi-1.0.5-5.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-7075bc4ff8
[SECURITY] Fedora 30 Update: fribidi-1.0.5-5.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-533a72fec5
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2020:0291
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4361
Truncate isolate_level to FRIBIDI_BIDI_MAX_EXPLICIT_LEVEL · fribidi/fribidi@034c6e9 · GitHub	Patch github.com text/html	MISC github.com/fribidi/fribidi/commit/034c6e9a1d296286305f4cfd1e0072b87
CVE-2019-18397	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2019-18397
GNU FriBidi: Heap-based buffer overflow (GLSA 202003-41) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202003-41
'[oss-security] CVE-2019-18397 - Stack buffer overflow in GNU FriBidi >= 1.0.0' - MARC	Third Party Advisory marc.info text/html	MISC marc.info/?l=oss-security&m=157322128105807&w=2
#944327 - fribidi: CVE-2019-18397 - Debian Bug report logs	Issue Tracking Third Party Advisory bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=944327
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:4326

Related QID Numbers

376906 Alibaba Cloud Linux Security Update for fribidi (ALINUX2-SA-2020:0004)

500193 Alpine Linux Security Update for fribidi

750026 SUSE Enterprise Linux Security Update for fribidi (SUSE-SU-2021:1655-1)

750202 OpenSUSE Security Update for fribidi (openSUSE-SU-2021:0763-1)

750783 OpenSUSE Security Update for fribidi (openSUSE-SU-2021:1655-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All

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	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnu	Fribidi	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

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:10.0:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:gnu:fribidi:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→