CVE-2011-0020

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2011-0020
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-24 18:00:00 UTC
Updated	2023-02-13 03:22:00 UTC
Description	Heap-based buffer overflow in the pango_ft2_font_render_box_glyph function in pango/pangoft2-render.c in libpango in Pa

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Pango	1.28.0	All	All	All
Application	Gnome	Pango	1.28.1	All	All	All
Application	Gnome	Pango	1.28.2	All	All	All
Application	Gnome	Pango	All	All	All	All
Application	Pango	Pango	0.20	All	All	All
Application	Pango	Pango	0.21	All	All	All
Application	Pango	Pango	0.22	All	All	All
Application	Pango	Pango	0.23	All	All	All
Application	Pango	Pango	0.24	All	All	All
Application	Pango	Pango	0.25	All	All	All
Application	Pango	Pango	0.26	All	All	All
Application	Pango	Pango	1.0	All	All	All
Application	Pango	Pango	1.1	All	All	All
Application	Pango	Pango	1.10	All	All	All
Application	Pango	Pango	1.11	All	All	All
Application	Pango	Pango	1.12	All	All	All
Application	Pango	Pango	1.13	All	All	All

Application	Pango	Pango	1.14	All	All	All
Application	Pango	Pango	1.15	All	All	All
Application	Pango	Pango	1.16	All	All	All
Application	Pango	Pango	1.17	All	All	All
Application	Pango	Pango	1.18	All	All	All
Application	Pango	Pango	1.19	All	All	All
Application	Pango	Pango	1.2	All	All	All
Application	Pango	Pango	1.20	All	All	All
Application	Pango	Pango	1.21	All	All	All
Application	Pango	Pango	1.22	All	All	All
Application	Pango	Pango	1.23	All	All	All
Application	Pango	Pango	1.24	All	All	All
Application	Pango	Pango	1.25	All	All	All
Application	Pango	Pango	1.26	All	All	All
Application	Pango	Pango	1.27	All	All	All
Application	Pango	Pango	1.28.0	All	All	All
Application	Pango	Pango	1.28.1	All	All	All
Application	Pango	Pango	1.28.2	All	All	All
Application	Pango	Pango	1.3	All	All	All
Application	Pango	Pango	1.4	All	All	All
Application	Pango	Pango	1.5	All	All	All
Application	Pango	Pango	1.6	All	All	All
Application	Pango	Pango	1.7	All	All	All
Application	Pango	Pango	1.8	All	All	All
Application	Pango	Pango	1.9	All	All	All
Application	Pango	Pango	0.20	All	All	All
Application	Pango	Pango	0.21	All	All	All
Application	Pango	Pango	0.22	All	All	All
Application	Pango	Pango	0.23	All	All	All
Application	Pango	Pango	0.24	All	All	All
Application	Pango	Pango	0.25	All	All	All
Application	Pango	Pango	0.26	All	All	All
Application	Pango	Pango	1.0	All	All	All
Application	Pango	Pango	1.1	All	All	All
Application	Pango	Pango	1.10	All	All	All

Application	Pango	Pango	1.11	All	All	All
Application	Pango	Pango	1.12	All	All	All
Application	Pango	Pango	1.13	All	All	All
Application	Pango	Pango	1.14	All	All	All
Application	Pango	Pango	1.15	All	All	All
Application	Pango	Pango	1.16	All	All	All
Application	Pango	Pango	1.17	All	All	All
Application	Pango	Pango	1.18	All	All	All
Application	Pango	Pango	1.19	All	All	All
Application	Pango	Pango	1.2	All	All	All
Application	Pango	Pango	1.20	All	All	All
Application	Pango	Pango	1.21	All	All	All
Application	Pango	Pango	1.22	All	All	All
Application	Pango	Pango	1.23	All	All	All
Application	Pango	Pango	1.24	All	All	All
Application	Pango	Pango	1.25	All	All	All
Application	Pango	Pango	1.26	All	All	All
Application	Pango	Pango	1.27	All	All	All
Application	Pango	Pango	1.28.0	All	All	All
Application	Pango	Pango	1.28.1	All	All	All
Application	Pango	Pango	1.28.2	All	All	All
Application	Pango	Pango	1.3	All	All	All
Application	Pango	Pango	1.4	All	All	All
Application	Pango	Pango	1.5	All	All	All
Application	Pango	Pango	1.6	All	All	All
Application	Pango	Pango	1.7	All	All	All
Application	Pango	Pango	1.8	All	All	All
Application	Pango	Pango	1.9	All	All	All
Application	Pango	Pango	All	All	All	All

References

Reference	Source	L
Webmail - OVH	VUPEN	w
Pango "pango_ft2_font_render_box_glyph()" Buffer Overflow Vulnerability - Secunia.com	SECUNIA	s
Pango Font Parsing 'pangoft2-render.c' Heap Corruption Vulnerability	BID	w
Bug 639882 – Heap corruption in font parsing with FreeType2 backend	MISC	b

Support	REDHAT	w
Red Hat update for pango and evolution28-pango - Secunia.com	SECUNIA	s
Bug 671122 – CVE-2011-0020 pango: Heap-based buffer overflow by rendering glyph box for certain FT_Bitmap objects	CONFIRM	b
IBM X-Force Exchange	XF	e
access.redhat.com | CVE-2011-0020	MISC	a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	w
oss-security - CVE request: heap corruption in libpango	MLIST	o
oss-security - Re: CVE request: heap corruption in libpango	MLIST	o
Pango Heap Overflow in pango_ft2_font_render_box_glyph() Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	w
70596	OSVDB	o
Red Hat Customer Portal	MISC	a
Bug #696616 “Heap corruption in font parsing with FreeType2 back...” : Bugs : pango1.0 package : Ubuntu	CONFIRM	b
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	SUSE	li
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.