CVE-2013-6836

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-6836
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-12-19 04:24:00 UTC
Updated	2016-12-31 02:59:00 UTC
Description	Heap-based buffer overflow in the ms_escher_get_data function in plugins/excel/ms-escher.c in GNOME Office Gnumeric b

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Gnumeric	1.12.0	All	All	All
Application	Gnome	Gnumeric	1.12.1	All	All	All
Application	Gnome	Gnumeric	1.12.2	All	All	All
Application	Gnome	Gnumeric	1.12.3	All	All	All
Application	Gnome	Gnumeric	1.12.4	All	All	All
Application	Gnome	Gnumeric	1.12.5	All	All	All
Application	Gnome	Gnumeric	1.12.6	All	All	All
Application	Gnome	Gnumeric	1.12.7	All	All	All
Application	Gnome	Gnumeric	1.12.0	All	All	All
Application	Gnome	Gnumeric	1.12.1	All	All	All
Application	Gnome	Gnumeric	1.12.2	All	All	All
Application	Gnome	Gnumeric	1.12.3	All	All	All
Application	Gnome	Gnumeric	1.12.4	All	All	All
Application	Gnome	Gnumeric	1.12.5	All	All	All
Application	Gnome	Gnumeric	1.12.6	All	All	All
Application	Gnome	Gnumeric	1.12.7	All	All	All
Application	Gnome	Gnumeric	All	All	All	All

References

Reference	Source	Link	Tags
xls: fuzzed file crash. (b5480b69) · Commits · GNOME / gnumeric · GitLab	CONFIRM	git.gnome.org	Exploi
Bug 712772 – Heap-buffer-overflow in ms_escher_get_data on a fuzzed xls file	CONFIRM	bugzilla.gnome.org	Exploi
openSUSE-SU-2014:0201-1: moderate: update for gnumeric	SUSE	lists.opensuse.org	
Security Advisory SA56678 - SUSE update for gnumeric - Secunia	SECUNIA	secunia.com	
GNOME Office / Gnumeric - Gnumeric 1.12.9	CONFIRM	projects.gnome.org	Vendc
Gnome Gnumeric 'ms_escher_get_data()' Function Heap Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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