CVE-2014-3564

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

Summary

CVE	CVE-2014-3564
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-20 17:55:00 UTC
Updated	2023-02-13 00:40:00 UTC
Description	Multiple heap-based buffer overflows in the status_handler function in (1) engine-gpgsm.c and (2) engine-uiserver.c in GPG

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	10.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Application	Gnu	Gpgme	All	All	All	All

References

Reference	Source	Link	Tags
Oracle Solaris Third Party Bulletin - October 2015	CONFIRM	www.oracle.com	
Debian -- Security Information -- DSA-3005-1 gpgme1.0	DEBIAN	www.debian.org	
109699	OSVDB	www.osvdb.org	
oss-sec: CVE-2014-3564 gpgme: heap-based buffer overflow in gpgsm status handler	MLIST	seclists.org	
git.gnupg.org Git - gpgme.git/commit	MISC	git.gnupg.org	
git.gnupg.org Git - gpgme.git/commit	CONFIRM	git.gnupg.org	Patch
GPGME 'status_handler()' Function Heap Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	

Bug 1113267 – CVE-2014-3564 gpgme: heap-based buffer overflow in gpgsm status handler	CONFIRM	bugzilla.redhat.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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