CVE-2013-4576

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

Summary

CVE	CVE-2013-4576
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-12-20 21:55:06 UTC
Updated	2026-04-29 01:13:23 UTC
Description	GnuPG 1.x before 1.4.16 generates RSA keys using sequences of introductions with certain patterns that introduce a side c

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

AV:L/AC:L/Au:N/C:P/I:N/A:N

EPSS: 0.001080000 probability, percentile 0.286660000 (date 2026-04-30)

Problem Types: CWE-255 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Gnupg	Gnupg	1.0.0	All	All	All
Application	Gnupg	Gnupg	1.0.1	All	All	All
Application	Gnupg	Gnupg	1.0.2	All	All	All
Application	Gnupg	Gnupg	1.0.3	All	All	All
Application	Gnupg	Gnupg	1.0.4	All	All	All
Application	Gnupg	Gnupg	1.0.4	-	win32	All
Application	Gnupg	Gnupg	1.0.5	All	All	All
Application	Gnupg	Gnupg	1.0.5	-	win32	All
Application	Gnupg	Gnupg	1.0.6	All	All	All
Application	Gnupg	Gnupg	1.0.7	All	All	All
Application	Gnupg	Gnupg	1.2.0	All	All	All
Application	Gnupg	Gnupg	1.2.1	All	All	All
Application	Gnupg	Gnupg	1.2.1	windows	All	All
Application	Gnupg	Gnupg	1.2.2	All	All	All
Application	Gnupg	Gnupg	1.2.3	All	All	All
Application	Gnupg	Gnupg	1.2.4	All	All	All
Application	Gnupg	Gnupg	1.2.5	All	All	All
Application	Gnupg	Gnupg	1.2.6	All	All	All
Application	Gnupg	Gnupg	1.2.7	All	All	All
Application	Gnupg	Gnupg	1.3.0	All	All	All
Application	Gnupg	Gnupg	1.3.1	All	All	All
Application	Gnupg	Gnupg	1.3.2	All	All	All
Application	Gnupg	Gnupg	1.3.3	All	All	All
Application	Gnupg	Gnupg	1.3.4	All	All	All
Application	Gnupg	Gnupg	1.3.6	All	All	All
Application	Gnupg	Gnupg	1.3.90	All	All	All
Application	Gnupg	Gnupg	1.3.91	All	All	All
Application	Gnupg	Gnupg	1.3.92	All	All	All
Application	Gnupg	Gnupg	1.3.93	All	All	All
Application	Gnupg	Gnupg	1.4	All	All	All
Application	Gnupg	Gnupg	1.4.0	All	All	All
Application	Gnupg	Gnupg	1.4.10	All	All	All
Application	Gnupg	Gnupg	1.4.11	All	All	All
Application	Gnupg	Gnupg	1.4.12	All	All	All
Application	Gnupg	Gnupg	1.4.13	All	All	All
Application	Gnupg	Gnupg	1.4.14	All	All	All

Application	Gnupg	Gnupg	1.4.14	All	All	All
Application	Gnupg	Gnupg	1.4.2	All	All	All
Application	Gnupg	Gnupg	1.4.3	All	All	All
Application	Gnupg	Gnupg	1.4.4	All	All	All
Application	Gnupg	Gnupg	1.4.5	All	All	All
Application	Gnupg	Gnupg	1.4.6	All	All	All
Application	Gnupg	Gnupg	1.4.8	All	All	All
Application	Gnupg	Gnupg	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Debian -- Security Information -- DSA-2821-1 gnupg	af854a3a-2127-422b-91ae-364da2661
[Announce] [security fix] GnuPG 1.4.16 released	af854a3a-2127-422b-91ae-364da2661
www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf	af854a3a-2127-422b-91ae-364da2661
GnuPG Acoustic Side-Channel Attack Lets Local Users Recover RSA Secret Keys - SecurityTracker	af854a3a-2127-422b-91ae-364da2661
USN-2059-1: GnuPG vulnerability | Ubuntu	af854a3a-2127-422b-91ae-364da2661
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661
osvdb.org/101170	af854a3a-2127-422b-91ae-364da2661
oss-sec: Re: GnuPG 1.4.16 fixes RSA key extraction via acoustic side channel (CVE-2013-4576)	af854a3a-2127-422b-91ae-364da2661
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661
GnuPG RSA Key Extraction Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da2661
oss-sec: GnuPG 1.4.16 fixes RSA key extraction via acoustic side channel (CVE-2013-4576)	af854a3a-2127-422b-91ae-364da2661
Acoustic cryptanalysis	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report