CVE-2003-0971

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2003-0971
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-12-15 05:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	GnuPG (GPG) 1.0.2, and other versions up to 1.2.3, creates ElGamal type 20 (sign+encrypt) keys using the same key com

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Privacy Guard	1.0.2	All	All	All
Application	Gnu	Privacy Guard	1.0.3	All	All	All
Application	Gnu	Privacy Guard	1.0.3b	All	All	All
Application	Gnu	Privacy Guard	1.0.4	All	All	All
Application	Gnu	Privacy Guard	1.0.5	All	All	All
Application	Gnu	Privacy Guard	1.0.6	All	All	All
Application	Gnu	Privacy Guard	1.0.7	All	All	All
Application	Gnu	Privacy Guard	1.2	All	All	All
Application	Gnu	Privacy Guard	1.2.1	All	All	All
Application	Gnu	Privacy Guard	1.2.2	All	All	All
Application	Gnu	Privacy Guard	1.2.2	rc1	All	All
Application	Gnu	Privacy Guard	1.2.3	All	All	All
Application	Gnu	Privacy Guard	1.0.2	All	All	All
Application	Gnu	Privacy Guard	1.0.3	All	All	All
Application	Gnu	Privacy Guard	1.0.3b	All	All	All
Application	Gnu	Privacy Guard	1.0.4	All	All	All
Application	Gnu	Privacy Guard	1.0.5	All	All	All

Application	Gnu	Privacy Guard	1.0.6	All	All	All
Application	Gnu	Privacy Guard	1.0.7	All	All	All
Application	Gnu	Privacy Guard	1.2	All	All	All
Application	Gnu	Privacy Guard	1.2.1	All	All	All
Application	Gnu	Privacy Guard	1.2.2	All	All	All
Application	Gnu	Privacy Guard	1.2.2	rc1	All	All
Application	Gnu	Privacy Guard	1.2.3	All	All	All

References

Reference	Source	Link	Tags
Secunia - Advisories - GnuPG ElGamal Signing Weakness Expose Private Key	SECUNIA	secunia.com	
Secunia - Advisories - Fedora update for gnupg	SECUNIA	secunia.com	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	
Secunia - Advisories - SuSE update for gpg	SECUNIA	secunia.com	
NOVELL: Broken Link - 404 Error Pages	SUSE	www.novell.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
Secunia - Advisories - Red Hat update for gnupg	SECUNIA	secunia.com	
[Announce] GnuPG 1.2.3 patch to remove ElGamal signing keys	CONFIRM	lists.gnupg.org	Patch
Mandriva Security Advisories	MANDRAKE	www.mandriva.com	
'GnuPG's ElGamal signing keys compromised' - MARC	BUGTRAQ	marc.info	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	
Debian -- Security Information -- DSA-429-1 gnupg	DEBIAN	www.debian.org	
CERT/CC Vulnerability Note VU#940388	CERT-VN	www.kb.cert.org	US Government F
GnuPG ElGamal Signing Key Private Key Compromise Vulnerability	BID	www.securityfocus.com	Patch, Vendor Ac
20040202-01-U	SGI	patches.sgi.com	
[Announce] GnuPG's ElGamal signing keys compromised	CONFIRM	lists.gnupg.org	Patch, Vendor Ac
Home - Conectiva	CONECTIVA	distro.conectiva.com.br	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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

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