CVE-2009-1416

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

Summary

CVE	CVE-2009-1416
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-30 20:30:00 UTC
Updated	2009-06-10 05:29:00 UTC
Description	lib/gnutls_pk.c in libgnutls in GnuTLS 2.5.0 through 2.6.5 generates RSA keys stored in DSA structures, instead of the inter

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	2.5.0	All	All	All
Application	Gnu	Gnutls	2.6.0	All	All	All
Application	Gnu	Gnutls	2.6.1	All	All	All
Application	Gnu	Gnutls	2.6.2	All	All	All
Application	Gnu	Gnutls	2.6.3	All	All	All
Application	Gnu	Gnutls	2.6.4	All	All	All
Application	Gnu	Gnutls	2.6.5	All	All	All
Application	Gnu	Gnutls	2.5.0	All	All	All
Application	Gnu	Gnutls	2.6.0	All	All	All
Application	Gnu	Gnutls	2.6.1	All	All	All
Application	Gnu	Gnutls	2.6.2	All	All	All
Application	Gnu	Gnutls	2.6.3	All	All	All
Application	Gnu	Gnutls	2.6.4	All	All	All
Application	Gnu	Gnutls	2.6.5	All	All	All

References

Reference	Source	Link

Support / Security / Advisories / / MDVSA-2009:116 | Mandriva	MANDRIVA	www.mandriva.com
[Help-gnutls] Encryption using DSA keys	MLIST	lists.gnu.org
Gentoo Linux Documentation -- GnuTLS: Multiple vulnerabilities	GENTOO	security.gentoo.org
GnuTLS Prior to 2.6.6 Multiple Remote Vulnerabilities	BID	www.securityfocus.c
Webmail - OVH	VUPEN	www.vupen.com
GnuTLS Multiple Vulnerabilities - Secunia.com	SECUNIA	secunia.com
Gmane -- Mail To News And Back Again	MLIST	article.gmane.org
SecurityTracker.com Archives - GnuTLS DSA Key Generation Creates RSA Keys Instead of DSA Keys	SECTRACK	www.securitytracker.
Gentoo update for gnutls - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-09-21	Tomas Hoger	Not vulnerable. This issue did not affect versions of gnutls shipped in Red Hat Enterprise Linux

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