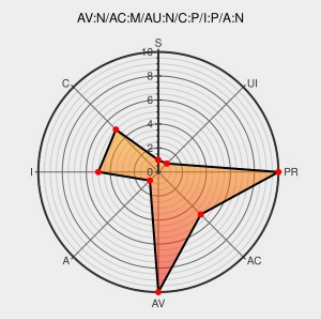
CVE-2009-5138

Published on: 03/06/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:27 PM UTC

CVE-2009-5138

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gnutls from Gnu contain the following vulnerability:

GnuTLS before 2.7.6, when the GNUTLS_VERIFY_ALLOW_X509_V1_CA_CRT flag is not enabled, treats version 1 X.509 certificates as intermediate CAs, which allows remote attackers to bypass intended restrictions by leveraging a X.509 V1 certificate from a trusted CA to issue new certificates, a different vulnerability than CVE-2014-1959.

CVE-2009-5138 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2014:0320-1: critical: Security update for g	lists.opensuse.org, text/html	SUSE SUSE-SU-2014:0320
Security Advisory SA57274 - SUSE update for gnutls - Secunia	web.archive.org, text/html	SECUNIA 57274
Security Advisory SA57254 - SUSE update for gnutls - Secunia	web.archive.org, text/html	SECUNIA 57254
[security-announce] SUSE-SU-2014:0445-1: important: Security update for	lists.opensuse.org, text/html	SUSE SUSE-SU-2014:0445

thread.gmane.org | 522: Connection timed out	thread.gmane.org text/html Inactive Link Not Archived	MLIST [oss-security] 20140227 Re: CVE Request - GnuTLS corrects flaw in certificate verification (3.1.x/3.2.x)
gitorious.org Git - gnutls:gnutls.git/commit	Exploit Patch web.archive.org text/xml Inactive Link Not Archived	CONFIRM gitorious.org/gnutls/gnutls/commit/c8dcbedd1fdc312f5b1a70fcfbc1afe235d800cd
thread.gmane.org | 522: Connection timed out	thread.gmane.org text/html Inactive Link Not Archived	MLIST [gnutls-devel] 20090109 Re: gnutls fails to use Verisign CA cert without a Basic Constraint
[security-announce] SUSE-SU-2014:0319-1: critical: Security update for g	lists.opensuse.org text/html	SUSE SUSE-SU-2014:0319
Security Advisory SA57321 - Red Hat update for gnutls - Secunia	web.archive.org text/html	SECUNIA 57321
Bug 1069301 – CVE-2009-5138 gnutls: incorrect handling of V1 intermediate certificates	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1069301
[security-announce] SUSE-SU-2014:0322-1: critical: Security update for g	lists.opensuse.org text/html	SUSE SUSE-SU-2014:0322
Security Advisory SA57260 - SUSE update for gnutls - Secunia	web.archive.org text/html	SECUNIA 57260
article.gmane.org | 522: Connection timed out	article.gmane.org text/html Inactive Link Not Archived	MLIST [oss-security] 20140225 Re: Re: CVE Request - GnuTLS corrects flaw in certificate verification (3.1.x/3.2.x)
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0247

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	2.7.0	All	All	All
Application	Gnu	Gnutls	2.7.1	All	All	All
Application	Gnu	Gnutls	2.7.2	All	All	All
Application	Gnu	Gnutls	2.7.3	All	All	All
Application	Gnu	Gnutls	2.7.4	All	All	All

Application	Gnu	Gnutls	2.7.0	All	All	All
Application	Gnu	Gnutls	2.7.1	All	All	All
Application	Gnu	Gnutls	2.7.2	All	All	All
Application	Gnu	Gnutls	2.7.3	All	All	All
Application	Gnu	Gnutls	2.7.4	All	All	All
Application	Gnu	Gnutls	All	All	All	All

cpe:2.3:a:gnu:gnutls:2.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.3:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.4:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.0:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.2:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.3:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:2.7.4:*:*:*:*:*:*:*:

cpe:2.3:a:gnu:gnutls:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→