

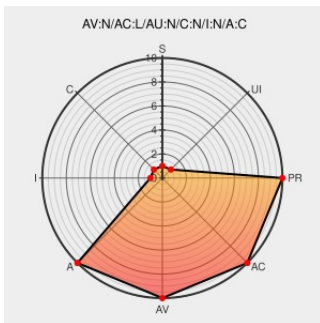


CVE-2004-2531

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2004-2531

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Gnutls](#) from [Gnu](#) contain the following vulnerability:
X.509 Certificate Signature Verification in Gnu transport layer security library (GnuTLS) 1.0.16 allows remote attackers to cause a denial of service (CPU consumption) via certificates containing long chains and signed with large RSA keys.

CVE-2004-2531 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
text/html

[XF gnutls-rsa-key-size-dos\(16858\)](#)

SecurityTracker.com Archives - GnuTLS X.509 Certificate Chain Validation Process Lets Remote Users Deny Service

[Patch](#)
[Vendor Advisory](#)
[securitytracker.com](https://securitytracker.com/text/html)
text/html

[SECTrack 1010838](#)

Gnu Transport Layer Security Library X.509 Certificate Verification Denial Of Service Vulnerability

[Patch](#)
[cve.report \(archive\)](#)
text/html

[BID 10839](#)

No Description Provided

[Patch](#)
www.osvdb.org

[OSVDB 8278](#)

Inactive Link Not Archived

[gnutls-dev] gnutls 1.0.17

lists.gnupg.org
text/html

MLIST [gnutls-dev]
20040802 gnutls
1.0.17

Secunia - Advisories - GnuTLS X.509 Certificate Signature Verification Denial of Service

Patch
Vendor Advisory
web.archive.org
text/html

SECUNIA 12156

Patch
Vendor Advisory
www.hornik.sk
text/plain

MISC
www.hornik.sk/SA/SA-20040802.txt

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	1.0.16	All	All	All
Application	Gnu	Gnutls	1.0.16	All	All	All
cpe:2.3:a:gnu:gnutls:1.0.16:*****:						
cpe:2.3:a:gnu:gnutls:1.0.16:*****:						

No vendor comments have been submitted for this CVE