



CVE-2015-0282

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-0282
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-24 17:59:00 UTC
Updated	2018-01-05 02:29:00 UTC
Description	GnuTLS before 3.1.0 does not verify that the RSA PKCS #1 signature algorithm matches the signature algorithm in the cert

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	All	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	rhn.redha
Debian -- Security Information -- DSA-3191-1 gnutls26	DEBIAN	www.debi
GnuTLS	CONFIRM	www.gnut
GnuTLS CVE-2015-0282 Certificate Validation Security Bypass Vulnerability	BID	www.secu
GnuTLS Certificate Validation Flaw Lets Remote Users Force a Signature Algorithm Downgrade - SecurityTracker	SECTrack	www.secu
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)