



CVE-2016-7444

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

Summary

CVE	CVE-2016-7444
State	PUBLISHED
Assigner	debian
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-27 15:59:12 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

EPSS: 0.010210000 probability, percentile 0.773520000 (date 2026-05-07)

Problem Types: CWE-264 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

High

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	3.5.0	All	All	All
Application	Gnu	Gnutls	3.5.1	All	All	All
Application	Gnu	Gnutls	3.5.2	All	All	All
Application	Gnu	Gnutls	3.5.3	All	All	All
Application	Gnu	Gnutls	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References	
Reference	Source
ocsp: corrected the comparison of the serial size in OCSP response (964632f3) · Commits · gnutls / Gnutls · GitLab	af854a3a-2127-422b-91
GnuTLS	af854a3a-2127-422b-91
Red Hat Customer Portal	af854a3a-2127-422b-91
GnuTLS GNUTLS-SA-2016-3 Certificate Validation Security Bypass Vulnerability	af854a3a-2127-422b-91
[gnutls-devel] OCSP certificate check	af854a3a-2127-422b-91

[ignore CVEs] CVE: estimate check	also read CVE: 1234 567
[security-announce] openSUSE-SU-2017:0386-1: important: Security update	af854a3a-2127-422b-91
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings	
672230 EulerOS Security Update for gnutls (EulerOS-SA-2022-2609)	

© [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](#)