Gnutls: gnutls impacted by inefficient der decoding in libtasn1 leading to remote dos

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

Summary

CVE	CVE-2024-12243
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-10 16:15:37 UTC
Updated	2026-05-12 12:16:17 UTC
Description	A flaw was found in GnuTLS, which relies on libtasn1 for ASN.1 data processing. Due to an inefficient algorithm in libtasn1,

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

EPSS: 0.012270000 probability, percentile 0.792870000 (date 2026-05-12)

Problem Types: CWE-407 | CWE-407 Inefficient Algorithmic Complexity

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

vailability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.6.16-8.el8_10.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.6.16-8.el8_10.3 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.8.3-6.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.8.3-6.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:3.7.6-21.el9_2.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:3.8.3-4.el9_4.2 * rpm
CNA	Red Hat	Red Hat Discovery 1.14	unaffected sha256:ad1045aa0de937c3a6969ec377
CNA	Red Hat	Red Hat Discovery 1.14	unaffected sha256:c960fa13577db72b52765d69416
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom
ADP	Siemens	RUGGEDCOM ROX MX5000	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX MX5000RE	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1400	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1500	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1501	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1510	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1511	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1512	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1524	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX1536	affected V2.17.0 custom
ADP	Siemens	RUGGEDCOM ROX RX5000	affected V2.17.0 custom

References

Reference	Source	Link	Tags
access.redhat.com/security/cve/CVE-2024-12243	secalert@redhat.com	access.redhat.com	
gitlab.com/gnutls/gnutls/-/issues/1553	secalert@redhat.com	gitlab.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
security.netapp.com/advisory/ntap-20250523-0002	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com	
access.redhat.com/errata/RHSA-2025:17361	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:4051	secalert@redhat.com	access.redhat.com	
cert-portal.siemens.com/productcert/html/ssa-202008.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
gitlab.com/gnutls/libtasn1/-/issues/52	secalert@redhat.com	gitlab.com	
access.redhat.com/errata/RHSA-2025:8385	secalert@redhat.com	access.redhat.com	
lists.debian.org/debian-lts-announce/2025/02/msg00027.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/errata/RHSA-2025:8020	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:7076	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Bing Shi for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-02-10T08:33:56.422Z	Reported to Red Hat.
CNA	2025-02-10T00:00:00.000Z	Made public.

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

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