



# Libtasn1: inefficient der decoding in libtasn1 leading to potential remote dos

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

## Summary

<b>CVE</b>	CVE-2024-12133
<b>State</b>	PUBLISHED
<b>Assigner</b>	redhat
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-02-10 16:15:37 UTC
<b>Updated</b>	2026-05-12 12:16:16 UTC

**Description** A flaw in libtasn1 causes inefficient handling of specific certificate data. When processing a large number of elements in a c

## 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:** 0.003430000 probability, percentile 0.569390000 (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

Integrity

None

Availability

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 0:4.13-5.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:4.13-5.el8_10 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:4.16.0-9.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:4.16.0-9.el9 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:4.16.0-8.el9_2.1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:4.16.0-8.el9_4.1 * rpm
CNA	Red Hat	Red Hat Discovery 1.14	unaffected sha256:ad1045aa0de937c3a6969ec3771
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
<a href="http://www.openwall.com/lists/oss-security/2025/02/06/6">www.openwall.com/lists/oss-security/2025/02/06/6</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="http://cert-portal.siemens.com/productcert/html/ssa-082556.html">cert-portal.siemens.com/productcert/html/ssa-082556.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="http://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="http://lists.debian.org/debian-lts-announce/2025/02/msg00025.html">lists.debian.org/debian-lts-announce/2025/02/msg00025.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://lists.debian.org">lists.debian.org</a>
<a href="http://bugzilla.redhat.com/show_bug.cgi">bugzilla.redhat.com/show_bug.cgi</a>	secalert@redhat.com	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
<a href="http://access.redhat.com/errata/RHSA-2025:7077">access.redhat.com/errata/RHSA-2025:7077</a>	secalert@redhat.com	<a href="http://access.redhat.com">access.redhat.com</a>
<a href="https://gitlab.com/gnutls/libtasn1/-/blob/master/doc/security/CVE-2024-12133.md">gitlab.com/gnutls/libtasn1/-/blob/master/doc/security/CVE-2024-12133.md</a>	secalert@redhat.com	<a href="https://gitlab.com">gitlab.com</a>
<a href="http://access.redhat.com/errata/RHSA-2025:8021">access.redhat.com/errata/RHSA-2025:8021</a>	secalert@redhat.com	<a href="http://access.redhat.com">access.redhat.com</a>
<a href="http://security.netapp.com/advisory/ntap-20250523-0003">security.netapp.com/advisory/ntap-20250523-0003</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://security.netapp.com">security.netapp.com</a>
<a href="http://cert-portal.siemens.com/productcert/html/ssa-202008.html">cert-portal.siemens.com/productcert/html/ssa-202008.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="http://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="https://gitlab.com/gnutls/libtasn1/-/issues/52">gitlab.com/gnutls/libtasn1/-/issues/52</a>	secalert@redhat.com	<a href="https://gitlab.com">gitlab.com</a>
<a href="http://access.redhat.com/errata/RHSA-2025:8385">access.redhat.com/errata/RHSA-2025:8385</a>	secalert@redhat.com	<a href="http://access.redhat.com">access.redhat.com</a>
<a href="http://access.redhat.com/errata/RHSA-2025:4049">access.redhat.com/errata/RHSA-2025:4049</a>	secalert@redhat.com	<a href="http://access.redhat.com">access.redhat.com</a>
<a href="http://access.redhat.com/security/cve/CVE-2024-12133">access.redhat.com/security/cve/CVE-2024-12133</a>	secalert@redhat.com	<a href="http://access.redhat.com">access.redhat.com</a>
<a href="http://access.redhat.com/errata/RHSA-2025:17347">access.redhat.com/errata/RHSA-2025:17347</a>	secalert@redhat.com	<a href="http://access.redhat.com">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

## 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	2025-02-10T08:14:05.460Z	Reported to Red Hat.
CNA	2025-02-10T00:00:00.000Z	Made public.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)