



# CVE-2015-3622

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

## Summary

<b>CVE</b>	CVE-2015-3622
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-05-12 19:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.5 allows remote attackers to cause a deni

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Libtasn1</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All

## References

Reference	Source	Link
USN-2604-1: Libtasn1 vulnerability   Ubuntu	UBUNTU	<a href="#">www.ubuntu.com</a>
GNU Libtasn1 4.5 released	MLIST	<a href="#">lists.gnu.org</a>
[SECURITY] Fedora 21 Update: libtasn1-4.5-1.fc21	FEDORA	<a href="#">lists.fedoraprojec</a>
openSUSE-SU-2016:1674-1: moderate: Security update for libtasn1	SUSE	<a href="#">lists.opensuse.or</a>
GNU Libtasn1 'decoding.c' Heap Buffer Overflow Vulnerability	BID	<a href="#">www.securityfocu</a>
Support / Security / Advisories // MDVSA-2015:232   Mandriva	MANDRIVA	<a href="#">www.mandriva.co</a>
Full Disclosure: Heap overflow / invalid read in Libtasn1 before 4.5 (TFPA 005/2015)	FULLDISC	<a href="#">seclists.org</a>
openSUSE-SU-2015:1372-1: moderate: Security update for gnutils	SUSE	<a href="#">lists.opensuse.or</a>
openSUSE-SU-2016:1567-1: moderate: Security update for libtasn1	SUSE	<a href="#">lists.opensuse.or</a>

libtasn1 Heap Overflow ≈ Packet Storm	MISC	<a href="#">packetstormsecu</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.co</a>
Debian -- Security Information -- DSA-3256-1 libtasn1-6	DEBIAN	<a href="#">www.debian.org</a>
libtASN1 Heap Over-read in _asn1_extract_der_octet() Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="#">www.securitytrac</a>
Gentoo Security	GENTOO	<a href="#">security.gentoo.o</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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](#).

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