



CVE-2006-0645

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

Summary

CVE	CVE-2006-0645
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-10 18:06:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Tiny ASN.1 Library (libtasn1) before 0.2.18, as used by (1) GnuTLS 1.2.x before 1.2.10 and 1.3.x before 1.3.4, and (2) GNU

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

EPSS: 0.037210000 probability, percentile 0.879980000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

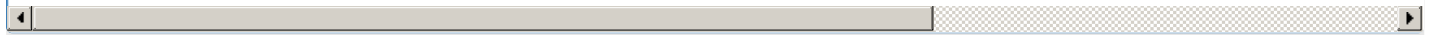
Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Free Software Foundation Inc.	Libtasn1	0.1.0	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.1.1	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.1.2	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.0	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.1	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.10	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.11	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.12	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.13	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.14	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.15	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.16	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.17	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.2	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.3	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.4	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.5	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.6	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.7	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.8	All	All	All
Application	Free Software Foundation Inc.	Libtasn1	0.2.9	All	All	All

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

References						
Reference					Source	
Advisories - Mandriva Linux					af854a3a-2127-422b-91ae-364da2f	
Repository / Oval Repository					af854a3a-2127-422b-91ae-364da2f	
USN-251-1: libtasn vulnerability Ubuntu security notices					af854a3a-2127-422b-91ae-364da2f	
[gnutls-dev] GnuTLS 1.3.4 - Experimental - Security release					af854a3a-2127-422b-91ae-364da2f	
GLEG Ltd. - Information Security Company					af854a3a-2127-422b-91ae-364da2f	
Fedora update for gnutls - Advisories - Secunia					af854a3a-2127-422b-91ae-364da2f	
GNUTLS LibTASN1 DER Decoding Denial of Service Vulnerabilities					af854a3a-2127-422b-91ae-364da2f	
SecurityTracker.com Archives - GnuTLS libtasn1 DER Decoding Bugs Let Remote Users Deny Service					af854a3a-2127-422b-91ae-364da2f	

Red Hat update for gnutls - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2f
SecurityFocus	af854a3a-2127-422b-91ae-364da2f
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2f
www.trustix.org/errata/2006/0008	af854a3a-2127-422b-91ae-364da2f
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2f
404 Not Found	af854a3a-2127-422b-91ae-364da2f
rhn.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2f
Ubuntu update for libtasn - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2f
GnuTLS libtasn1 DER Decoding Denial of Service Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2f
SecurityReason - libtasn vulnerability	af854a3a-2127-422b-91ae-364da2f
[gnutls-dev] GnuTLS 1.2.10 - Security release	af854a3a-2127-422b-91ae-364da2f
Mandriva update for gnutls - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2f
Repository - markup - gnupg-mirror: libtasn1/NEWS	af854a3a-2127-422b-91ae-364da2f
Gentoo Linux Documentation -- libtasn1, GNU TLS: Security flaw in DER decoding	af854a3a-2127-422b-91ae-364da2f
Gentoo update for libtasn1/gnutls - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2f
Debian update for libtasn1-2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da2f
Debian update for gnutls11 - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2f
www.osvdb.org/23054	af854a3a-2127-422b-91ae-364da2f
Debian -- Security Information -- DSA-985-1 libtasn1-2	af854a3a-2127-422b-91ae-364da2f
Debian -- Security Information -- DSA-986-1 gnutls11	af854a3a-2127-422b-91ae-364da2f
[SECURITY] Fedora Core 4 Update: gnutls-1.0.25-2.FC4	af854a3a-2127-422b-91ae-364da2f
404 Not Found	af854a3a-2127-422b-91ae-364da2f
[gnutls-dev] Libtasn1 0.2.18 - Tiny ASN.1 Library - Security release	af854a3a-2127-422b-91ae-364da2f
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



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