



CVE-2017-6891

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

Summary

CVE	CVE-2017-6891
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-22 19:29:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	Two errors in the "asn1_find_node()" function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be exploited to ca

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Bookkeeper	4.12.1	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Gnu	Gnutls Libtasn1	4.10	All	All	All
Application	Gnu	Gnutls Libtasn1	4.10	All	All	All
Application	Gnu	Libtasn1	4.10	All	All	All

References

Reference

Computer Security Research - Secunia
Savannah Git Hosting - libtasn1.git/commit
[bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade
GNU Libtasn1: Multiple vulnerabilities (GLSA 201710-11) — Gentoo security
Pony Mail!
[security-announce] openSUSE-SU-2019:1510-1: moderate: Security update f
Security Advisory SA76125 - GnuTLS libtasn1 "asn1_find_node()" Buffer Overflow Vulnerabilities - Secunia
Pony Mail!
[bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade

Savannah Git Hosting - libtasn1.git/commit

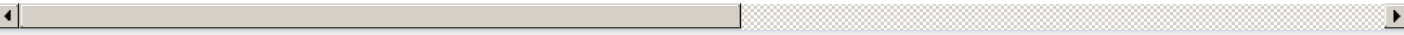
libtASN1 Stack Overflow in asn1_find_node() in Processing Assignment Files Lets Remote Users Execute Arbitrary Code - SecurityTracker

GnuTLS CVE-2017-6891 Stack Buffer Overflow Vulnerability

Debian -- Security Information -- DSA-3861-1 libtasn1-6

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710419](#) Gentoo Linux GNU Libtasn1 Multiple Vulnerabilities (GLSA 201710-11)

© [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](#)