



# CVE-2022-47629

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

## Summary

<b>CVE</b>	CVE-2022-47629
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-12-20 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:56:00 UTC
<b>Description</b>	Libksba before 1.6.3 is prone to an integer overflow vulnerability in the CRL signature parser.

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Libksba</a>	All	All	All	All
Application	<a href="#">Libksba Project</a>	<a href="#">Libksba</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="#">⚡ T6284 Another integer overflow in Libksba</a>	MISC	<a href="https://dev.gnupg.org">dev.gnupg.org</a>	
<a href="https://git.gnupg.org">git.gnupg.org</a> Git - libksba.git/commit	MISC	<a href="https://git.gnupg.org">git.gnupg.org</a>	
<a href="https://git.gnupg.org">git.gnupg.org</a> Git		<a href="https://git.gnupg.org">git.gnupg.org</a>	
[SECURITY] [DLA 3248-1] libksba security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
libksba: Remote Code Execution (GLSA 202212-07) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
Debian -- Security Information -- DSA-5305-1 libksba	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
CVE-2022-47629 Libksba Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analys

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[160442](#) Oracle Enterprise Linux Security Update for libksba (ELSA-2023-0530)

[160448](#) Oracle Enterprise Linux Security Update for libksba (ELSA-2023-0625)

[160450](#) Oracle Enterprise Linux Security Update for libksba (ELSA-2023-0626)

[181439](#) Debian Security Update for libksba (DSA 5305-1)

[181445](#) Debian Security Update for libksba (DLA 3248-1)

[184121](#) Debian Security Update for libksba (CVE-2022-47629)

[199083](#) Ubuntu Security Notification for Libksba Vulnerability (USN-5787-1)

[199534](#) Ubuntu Security Notification for Libksba Vulnerability (USN-5787-2)

[241145](#) Red Hat Update for libksba (RHSA-2023:0530)

[241167](#) Red Hat Update for libksba (RHSA-2023:0594)

[241168](#) Red Hat Update for libksba (RHSA-2023:0625)

[241171](#) Red Hat Update for libksba (RHSA-2023:0624)

[241173](#) Red Hat Update for libksba (RHSA-2023:0626)

[241175](#) Red Hat Update for libksba (RHSA-2023:0629)

[241640](#) Red Hat Update for libksba (RHSA-2023:0592)

[241686](#) Red Hat Update for libksba (RHSA-2023:0593)

[257220](#) CentOS Security Update for libksba (CESA-2023:0530)

[355091](#) Amazon Linux Security Advisory for libksba : ALAS2-2023-2041

[355346](#) Amazon Linux Security Advisory for libksba : ALAS-2023-1752

[355515](#) Amazon Linux Security Advisory for libksba : AL2012-2023-414

[377945](#) Alibaba Cloud Linux Security Update for libksba (ALINUX2-SA-2023:0009)

[377996](#) Alibaba Cloud Linux Security Update for libksba (ALINUX3-SA-2023:0021)

[502617](#) Alpine Linux Security Update for libksba

[502618](#) Alpine Linux Security Update for libksba

[502737](#) Alpine Linux Security Update for libksba

[505629](#) Alpine Linux Security Update for libksba

<a href="#">672745</a> EulerOS Security Update for libksba (EulerOS-SA-2023-1447)
<a href="#">672750</a> EulerOS Security Update for libksba (EulerOS-SA-2023-1472)
<a href="#">672785</a> EulerOS Security Update for libksba (EulerOS-SA-2023-1553)
<a href="#">672817</a> EulerOS Security Update for libksba (EulerOS-SA-2023-1528)
<a href="#">672923</a> EulerOS Security Update for libksba (EulerOS-SA-2023-1760)
<a href="#">672929</a> EulerOS Security Update for libksba (EulerOS-SA-2023-1782)
<a href="#">673103</a> EulerOS Security Update for libksba (EulerOS-SA-2023-2155)
<a href="#">710696</a> Gentoo Linux libksba Remote Code Execution Vulnerability (GLSA 202212-07)
<a href="#">753496</a> SUSE Enterprise Linux Security Update for libksba (SUSE-SU-2023:0031-1)
<a href="#">753527</a> SUSE Enterprise Linux Security Update for libksba (SUSE-SU-2023:0056-1)
<a href="#">753674</a> SUSE Enterprise Linux Security Update for libksba (SUSE-SU-2023:0031-2)
<a href="#">753708</a> SUSE Enterprise Linux Security Update for libksba (SUSE-SU-2023:0056-2)
<a href="#">904771</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (12106)
<a href="#">904772</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (12104)
<a href="#">905195</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (12106-1)
<a href="#">905239</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (12104-1)
<a href="#">940918</a> AlmaLinux Security Update for libksba (ALSA-2023:0625)
<a href="#">940923</a> AlmaLinux Security Update for libksba (ALSA-2023:0626)
<a href="#">960504</a> Rocky Linux Security Update for libksba (RLSA-2023:0626)
<a href="#">960518</a> Rocky Linux Security Update for libksba (RLSA-2023:0625)

© [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](#)