



# CVE-2022-3515

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

## Summary

<b>CVE</b>	CVE-2022-3515
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-12 15:15:00 UTC
<b>Updated</b>	2023-07-06 19:15:00 UTC
<b>Description</b>	A vulnerability was found in the Libksba library due to an integer overflow within the CRL parser. The vulnerability can be e

## Risk And Classification

### Problem Types: CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	All	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Gnupg</a>	All	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Libksba</a>	All	All	All	All
Application	<a href="#">Gnupg</a>	<a href="#">Vs-desktop</a>	All	All	All	All
Application	<a href="#">Gpg4win</a>	<a href="#">Gpg4win</a>	All	All	All	All
Application	<a href="#">Libksba Project</a>	<a href="#">Libksba</a>	All	All	All	All

## References

Reference	Source	Link
rK4b7d9cd4a018	MISC	<a href="#">dev.gnupg.org</a>
Security Advisory for Libksba/GnuPG (CVE-2022-3515)	MISC	<a href="#">www.gnupg.org</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access.redhat.com</a>
2135610 – (CVE-2022-3515) CVE-2022-3515 libksba: integer overflow may lead to remote code execution	MISC	<a href="#">bugzilla.redhat.com</a>
403 Forbidden	CONFIRM	<a href="#">security.netapp.com</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.

## Legacy QID Mappings

[160160](#) Oracle Enterprise Linux Security Update for libksba (ELSA-2022-7090)

[160162](#) Oracle Enterprise Linux Security Update for libksba (ELSA-2022-7088)

[160163](#) Oracle Enterprise Linux Security Update for libksba (ELSA-2022-7089)

[181139](#) Debian Security Update for libksba (DLA 3153-1)

[181140](#) Debian Security Update for libksba (DSA 5255-1)

[184118](#) Debian Security Update for libksba (CVE-2022-3515)

[198995](#) Ubuntu Security Notification for Libksba Vulnerability (USN-5688-1)

[199007](#) Ubuntu Security Notification for Libksba Vulnerability (USN-5688-2)

[240767](#) Red Hat Update for libksba (RHSA-2022:7089)

[240768](#) Red Hat Update for libksba (RHSA-2022:7088)

[240769](#) Red Hat Update for libksba (RHSA-2022:7090)

[240862](#) Red Hat Update for libksba (RHSA-2022:7927)

[257201](#) CentOS Security Update for libksba (CESA-2022:7088)

[283236](#) Fedora Security Update for libksba (FEDORA-2022-3ef41c3410)

[283269](#) Fedora Security Update for libksba (FEDORA-2022-7c13845b0d)

[283487](#) Fedora Security Update for libksba (FEDORA-2022-0002284730)

[354132](#) Amazon Linux Security Advisory for libksba : ALAS2-2022-1890

[354250](#) Amazon Linux Security Advisory for libksba : ALAS-2022-1649

[354418](#) Amazon Linux Security Advisory for libksba : ALAS2022-2022-249

[354543](#) Amazon Linux Security Advisory for libksba : ALAS-2022-249

[355054](#) Amazon Linux Security Advisory for libksba : AL2012-2022-378

[355266](#) Amazon Linux Security Advisory for libksba : ALAS2023-2023-088

[377712](#) Alibaba Cloud Linux Security Update for libksba (ALINUX2-SA-2022:0048)

[377716](#) Alibaba Cloud Linux Security Update for libksba (ALINUX3-SA-2022:0174)

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

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

502736 Alpine Linux Security Update for libksba
505628 Alpine Linux Security Update for libksba
672412 EulerOS Security Update for libksba (EulerOS-SA-2022-2797)
672741 EulerOS Security Update for libksba (EulerOS-SA-2023-1508)
672745 EulerOS Security Update for libksba (EulerOS-SA-2023-1447)
672750 EulerOS Security Update for libksba (EulerOS-SA-2023-1472)
672785 EulerOS Security Update for libksba (EulerOS-SA-2023-1553)
672817 EulerOS Security Update for libksba (EulerOS-SA-2023-1528)
672923 EulerOS Security Update for libksba (EulerOS-SA-2023-1760)
672929 EulerOS Security Update for libksba (EulerOS-SA-2023-1782)
710649 Gentoo Linux libksba Remote Code Execution Vulnerability (GLSA 202210-23)
710696 Gentoo Linux libksba Remote Code Execution Vulnerability (GLSA 202212-07)
752694 SUSE Enterprise Linux Security Update for libksba (SUSE-SU-2022:3683-1)
752698 SUSE Enterprise Linux Security Update for libksba (SUSE-SU-2022:3681-1)
905253 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (13001)
905255 Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (13004)
905262 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (13005)
905653 Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (13004-1)
906603 Common Base Linux Mariner (CBL-Mariner) Security Update for libksba (13004-3)
906640 Common Base Linux Mariner (CBL-Mariner) Security Update for gnupg2 (13005-3)
940712 AlmaLinux Security Update for libksba (ALSA-2022:7090)
940714 AlmaLinux Security Update for libksba (ALSA-2022:7089)
960243 Rocky Linux Security Update for libksba (RLSA-2022:7089)
960604 Rocky Linux Security Update for libksba (RLSA-2022:7090)

© 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)