



# CVE-2023-5992

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

## Summary

<b>CVE</b>	CVE-2023-5992
<b>State</b>	RESERVED
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-31 14:15:00 UTC
<b>Updated</b>	2024-03-16 03:15:00 UTC
<b>Description</b>	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openc Project</a>	<a href="#">Openc</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All

## References

Reference	Source	Link
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		<a href="#">lists.fe</a>
cve-details		<a href="#">acce</a>
RHSA-2024:0966		<a href="#">acce</a>
2248685 - (CVE-2023-5992) CVE-2023-5992 OpenSC: Side-channel leaks while stripping encryption PKCS#1 padding		<a href="#">bugzil</a>
CVE 2023 5992 · OpenSC/OpenSC Wiki · GitHub		<a href="#">github</a>
RHSA-2024:0967		<a href="#">acce</a>
lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/messag...		<a href="#">lists.fe</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.ni</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[161378](#) Oracle Enterprise Linux Security Update for opencs (ELSA-2024-0966)

[161382](#) Oracle Enterprise Linux Security Update for opencs (ELSA-2024-0967)

[242974](#) Red Hat Update for opencs (RHSA-2024:0967)

[242975](#) Red Hat Update for opencs (RHSA-2024:0966)

[285362](#) Fedora Security Update for opencs (FEDORA-2024-6460a03e29)

[285363](#) Fedora Security Update for opencs (FEDORA-2024-b92d44f141)

[357370](#) Amazon Linux Security Advisory for opencs : ALAS2023-2024-580

[379617](#) Alibaba Cloud Linux Security Update for opencs (ALINUX3-SA-2024:0026)

[941590](#) AlmaLinux Security Update for opencs (ALSA-2024:0967)

[941604](#) AlmaLinux Security Update for opencs (ALSA-2024:0966)

© [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](#)