



# CVE-2023-5678

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

## Summary

<b>CVE</b>	CVE-2023-5678
<b>State</b>	PUBLIC
<b>Assigner</b>	openssl-security@openssl.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-06 16:15:00 UTC
<b>Updated</b>	2023-11-30 22:15:00 UTC
<b>Description</b>	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters m

## Risk And Classification

**Problem Types:** CWE-754

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All

## References

Reference	Source	Link	Tags
git.openssl.org Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
security.netapp.com/advisory/ntap-20231130-0010		<a href="https://security.netapp.com">security.netapp.com</a>	
git.openssl.org Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
/err404.html	MISC	<a href="https://www.openssl.org">www.openssl.org</a>	
git.openssl.org Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
git.openssl.org Git - openssl.git/commitdiff	MISC	<a href="https://git.openssl.org">git.openssl.org</a>	
oss-security - OpenSSL Security Advisory	MISC	<a href="https://www.openwall.com">www.openwall.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, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">161251</a> Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2023-7877)
<a href="#">161287</a> Oracle Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ELSA-2024-12056)
<a href="#">200094</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6622-1)
<a href="#">200107</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6632-1)
<a href="#">200215</a> Ubuntu Security Notification for Open Secure Sockets Layer (OpenSSL) Vulnerabilities (USN-6709-1)
<a href="#">242632</a> Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:7877)
<a href="#">242687</a> Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2024:0154)
<a href="#">242696</a> Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2024:0208)
<a href="#">243077</a> Red Hat Update for JBoss Core Services (RHSA-2024:1316)
<a href="#">330164</a> IBM Advanced Interactive eXecutive (AIX) Open Secure Sockets Layer (OpenSSL) Multiple Vulnerabilities (openssl_advisory40)
<a href="#">356767</a> Amazon Linux Security Advisory for openssl11 : ALAS2-2023-2351
<a href="#">356770</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2-2023-2350
<a href="#">356780</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS-2023-1891
<a href="#">356891</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL)-snapsafe : ALAS2OPENSSL-SNAPSAFE-2023-004
<a href="#">356903</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : ALAS2023-2023-443
<a href="#">356993</a> Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL) : AL2012-2023-477
<a href="#">357333</a> Amazon Linux Security Advisory for edk2 : ALAS2-2024-2502
<a href="#">379545</a> Splunk Enterprise Third Party Package Updates for March 2024 (SVD-2024-0303)
<a href="#">379546</a> Splunk Universal Forwarder Third Party Package Updates for March 2024 (SVD-2024-0304)
<a href="#">379630</a> Alibaba Cloud Linux Security Update for Open Secure Sockets Layer (OpenSSL) (ALINUX3-SA-2024:0047)
<a href="#">503552</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">503621</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">503687</a> Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)
<a href="#">504259</a> Alpine Linux Security Update for openssl
<a href="#">505911</a> Alpine Linux Security Update for openssl
<a href="#">673338</a> EulerOS Security Update for shim (EulerOS-SA-2024-1098)
<a href="#">673343</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1125)
<a href="#">673443</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1069)

<a href="#">673480</a> EulerOS Security Update for shim (EulerOS-SA-2024-1129)
<a href="#">673598</a> EulerOS Security Update for compat-openssl10 (EulerOS-SA-2024-1258)
<a href="#">673684</a> EulerOS Security Update for shim (EulerOS-SA-2024-1164)
<a href="#">673687</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1184)
<a href="#">673724</a> EulerOS Security Update for shim (EulerOS-SA-2024-1299)
<a href="#">673737</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1287)
<a href="#">673773</a> EulerOS Security Update for linux-sgx (EulerOS-SA-2024-1124)
<a href="#">673790</a> EulerOS Security Update for shim (EulerOS-SA-2024-1186)
<a href="#">673797</a> EulerOS Security Update for shim-signed (EulerOS-SA-2024-1165)
<a href="#">673858</a> EulerOS Security Update for openssl111d (EulerOS-SA-2024-1157)
<a href="#">673889</a> EulerOS Security Update for shim (EulerOS-SA-2024-1113)
<a href="#">673908</a> EulerOS Security Update for shim (EulerOS-SA-2024-1206)
<a href="#">673915</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1155)
<a href="#">673962</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1204)
<a href="#">674007</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1093)
<a href="#">674055</a> EulerOS Security Update for Open Secure Sockets Layer (OpenSSL) (EulerOS-SA-2024-1109)
<a href="#">674097</a> EulerOS Security Update for shim (EulerOS-SA-2024-1074)
<a href="#">691351</a> Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (a5956603-7e4f-11ee-9df6-84a93843eb75)
<a href="#">755307</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4524-1)
<a href="#">755308</a> SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:4523-1)
<a href="#">755309</a> SUSE Enterprise Linux Security Update for openssl-1_0_0 (SUSE-SU-2023:4522-1)
<a href="#">755310</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4521-1)
<a href="#">755311</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4520-1)
<a href="#">755312</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4519-1)
<a href="#">755313</a> SUSE Enterprise Linux Security Update for openssl-1_1 (SUSE-SU-2023:4518-1)
<a href="#">755361</a> SUSE Enterprise Linux Security Update for compat-openssl098 (SUSE-SU-2023:4593-1)
<a href="#">755375</a> SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:4635-1)
<a href="#">755461</a> SUSE Enterprise Linux Security Update for openssl-3 (SUSE-SU-2023:4649-1)

[755503](#) SUSE Enterprise Linux Security Update for openssl-1\_1-livepatches (SUSE-SU-2023:4919-1)

[755504](#) SUSE Enterprise Linux Security Update for Open Secure Sockets Layer (OpenSSL)-1\_1-livepatches (SUSE-SU-2023:4918-1)

[907698](#) Common Base Linux Mariner (CBL-Mariner) Security Update for Open Secure Sockets Layer (OpenSSL) (31880-1)

[907730](#) Common Base Linux Mariner (CBL-Mariner) Security Update for edk2 (31872-1)

[941507](#) AlmaLinux Security Update for Open Secure Sockets Layer (OpenSSL) (ALSA-2023:7877)

© [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](#)