



Unbounded memory growth with session handling in TLSv1.3

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

Summary

CVE	CVE-2024-2511
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-08 14:15:07 UTC
Updated	2026-05-12 12:16:33 UTC
Description	Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from ADP

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.090520000 probability, percentile 0.926970000 (date 2026-05-12)

Problem Types: CWE-1325 | CWE-1325 CWE-1325 Improperly Controlled Sequential Memory Allocation

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSSL	OpenSSL	affected 3.2.0 3.2.2 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.1.0 3.1.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.14 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1y custom	Not specified
ADP	Siemens	RUGGEDCOM RM1224 LTE4G EU	affected V8.2 custom	Not specified
ADP	Siemens	RUGGEDCOM RM1224 LTE4G NAM	affected V8.2 custom	Not specified
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom	Not specified
ADP	Siemens	SCALANCE M804PB	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M812-1 ADSL-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M812-1 ADSL-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M816-1 ADSL-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M816-1 ADSL-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M826-2 SHDSL-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M874-2	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M874-3	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M874-3 3G-Router CN	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M876-3	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M876-3 ROK	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M876-4	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M876-4 EU	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE M876-4 NAM	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM853-1 A1	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM853-1 B1	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM853-1 EU	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM856-1 A1	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM856-1 B1	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM856-1 CN	affected V8.2 custom	Not specified

ADP	Siemens	SCALANCE MUM856-1 EU	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE MUM856-1 RoW	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE S615 EEC LAN-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE S615 LAN-Router	affected V8.2 custom	Not specified
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom	Not specified
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom	Not specified
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom	Not specified

References

Reference	Source	Lin
cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert
github.com/openssl/openssl/commit/7e4d731b1c07201ad9374c1cd9ac5263bdf35bce	af854a3a-2127-422b-91ae-364da2661108	gith
security.netapp.com/advisory/ntap-20240503-0013	af854a3a-2127-422b-91ae-364da2661108	sec
cert-portal.siemens.com/productcert/html/ssa-354112.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert
www.openssl.org/news/secadv/20240408.txt	af854a3a-2127-422b-91ae-364da2661108	ww
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert
cert-portal.siemens.com/productcert/html/ssa-769027.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert
cert-portal.siemens.com/productcert/html/ssa-915275.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert
github.com/openssl/openssl/extended-releases/commit/5f8d25770ae6437db119dfc951e2...	af854a3a-2127-422b-91ae-364da2661108	gith
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert
github.com/openssl/openssl/commit/e9d7083e241670332e0443da0f0d4ffb52829f08	af854a3a-2127-422b-91ae-364da2661108	gith
lists.debian.org/debian-lts-announce/2024/11/msg00000.html	af854a3a-2127-422b-91ae-364da2661108	lists
lists.debian.org/debian-lts-announce/2024/10/msg00033.html	af854a3a-2127-422b-91ae-364da2661108	lists
www.openwall.com/lists/oss-security/2024/04/08/5	af854a3a-2127-422b-91ae-364da2661108	ww
github.com/openssl/openssl/commit/b52867a9f618bb955bed2a3ce3db4d4f97ed8e5d	af854a3a-2127-422b-91ae-364da2661108	gith
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

CNA: Meriah Botider (Hewlett Packard Enterprise) (cna)

CNA: manish Patidar (Hewlett Packard Enterprise) (en)

CNA: Matt Caswell (en)

Legacy QID Mappings

38921 Open Secure Sockets Layer (OpenSSL) Denial of Service Vulnerability

510809 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

510810 Alpine Linux Security Update for Open Secure Sockets Layer (OpenSSL)

691472 Free Berkeley Software Distribution (FreeBSD) Security Update for Open Secure Sockets Layer (OpenSSL) (7c217849-f7d7-11ee-a490-84a93843eb75)

© [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](#)