



# SSL\_select\_next\_proto buffer overflow

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

## Summary

<b>CVE</b>	CVE-2024-5535
<b>State</b>	PUBLISHED
<b>Assigner</b>	openssl
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-06-27 11:15:24 UTC
<b>Updated</b>	2026-05-12 12:17:20 UTC
<b>Description</b>	Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer

## Risk And Classification

**Primary CVSS:** v3.1 9.1 CRITICAL from ADP

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

**Problem Types:** CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

High

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

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.3.0 3.3.2 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.2.0 3.2.3 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.1.0 3.1.7 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 3.0.0 3.0.15 semver	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 1.1.1 1.1.1za custom	Not specified
CNA	<a href="#">OpenSSL</a>	<a href="#">OpenSSL</a>	affected 1.0.2 1.0.2zk custom	Not specified
ADP	<a href="#">Openssl</a>	<a href="#">Openssl</a>	affected 3.3.0 3.3.2 custom	Not specified
ADP	<a href="#">Openssl</a>	<a href="#">Openssl</a>	affected 3.2.0 3.2.3 custom	Not specified
ADP	<a href="#">Openssl</a>	<a href="#">Openssl</a>	affected 3.1.0 3.1.7 custom	Not specified
ADP	<a href="#">Openssl</a>	<a href="#">Openssl</a>	affected 3.0.0 3.0.15 custom	Not specified
ADP	<a href="#">Openssl</a>	<a href="#">Openssl</a>	affected 1.1.1 1.1.1za custom	Not specified
ADP	<a href="#">Openssl</a>	<a href="#">Openssl</a>	affected 1.0.2 1.0.2zk custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">RUGGEDCOM RST2428P</a>	affected V3.1 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family</a>	unaffected * custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SCALANCE XCM-/XRM-/XCH-/XRH-300 Family</a>	affected V3.1 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIDIS Prime</a>	affected V4.0.700 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem</a>	affected * custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518-4 PN/DP MFP</a>	affected V3.1.0 V3.1.5 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518-4 PN/DP MFP</a>	affected V3.1.0 V3.1.5 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP</a>	affected V3.1.0 V3.1.5 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP</a>	affected V3.1.0 V3.1.5 custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIPLUS S7-1500 CPU 1518-4 PN/DP MFP</a>	affected V3.1.0 V3.1.5 custom	Not specified

## References

Reference	Source	Li
<a href="https://cert-portal.siemens.com/productcert/html/ssa-398330.html">cert-portal.siemens.com/productcert/html/ssa-398330.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
<a href="https://github.com/openssl/openssl/commit/99fb785a5f85315b95288921a321a935ea29a51e">github.com/openssl/openssl/commit/99fb785a5f85315b95288921a321a935ea29a51e</a>	af854a3a-2127-422b-91ae-364da2661108	git
<a href="https://security.netapp.com/advisory/ntap-20241025-0010">security.netapp.com/advisory/ntap-20241025-0010</a>	af854a3a-2127-422b-91ae-364da2661108	se
<a href="https://github.com/openssl/openssl/commit/e86ac436f0bd54d4517745483e2315650fae7b2c">github.com/openssl/openssl/commit/e86ac436f0bd54d4517745483e2315650fae7b2c</a>	af854a3a-2127-422b-91ae-364da2661108	git
<a href="https://github.com/openssl/openssl/commit/cf6f91f6121f4db167405db2f0de410a456f260c">github.com/openssl/openssl/commit/cf6f91f6121f4db167405db2f0de410a456f260c</a>	af854a3a-2127-422b-91ae-364da2661108	git

cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
www.openssl.org/news/secadv/20240627.txt	af854a3a-2127-422b-91ae-364da2661108	wv
cert-portal.siemens.com/productcert/html/ssa-769027.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
security.netapp.com/advisory/ntap-20241025-0006	af854a3a-2127-422b-91ae-364da2661108	se
cert-portal.siemens.com/productcert/html/ssa-915275.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
cert-portal.siemens.com/productcert/html/ssa-277137.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
www.openwall.com/lists/oss-security/2024/06/27/1	af854a3a-2127-422b-91ae-364da2661108	wv
github.openssl.org/openssl/extended-releases/commit/9947251413065a05189a63c9b7a6...	af854a3a-2127-422b-91ae-364da2661108	git
www.openwall.com/lists/oss-security/2024/06/28/4	af854a3a-2127-422b-91ae-364da2661108	wv
github.com/openssl/openssl/commit/4ada436a1946cbb24db5ab4ca082b69c1bc10f37	af854a3a-2127-422b-91ae-364da2661108	git
lists.debian.org/debian-lts-announce/2024/11/msg00000.html	af854a3a-2127-422b-91ae-364da2661108	lis
lists.debian.org/debian-lts-announce/2024/10/msg00033.html	af854a3a-2127-422b-91ae-364da2661108	lis
www.openwall.com/lists/oss-security/2024/08/15/1	af854a3a-2127-422b-91ae-364da2661108	wv
security.netapp.com/advisory/ntap-20240712-0005	af854a3a-2127-422b-91ae-364da2661108	se
github.openssl.org/openssl/extended-releases/commit/b78ec0824da857223486660177d3...	af854a3a-2127-422b-91ae-364da2661108	git
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

### Vendor Comments And Credit

Discovery Credit

**CNA:** Joseph Birr-Pixton (en)

**CNA:** David Benjamin (Google) (en)

**CNA:** Matt Caswell (en)

There are currently no legacy QID mappings associated with this CVE.

© 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](#)