



# Out-of-bounds read in HTTP client no\_proxy handling

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

## Summary

<b>CVE</b>	CVE-2025-9232
<b>State</b>	PUBLISHED
<b>Assigner</b>	openssl
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-30 14:15:41 UTC
<b>Updated</b>	2026-05-12 13:17:30 UTC

**Description** Issue summary: An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no\_

## 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:** 0.000390000 probability, percentile 0.117310000 (date 2026-05-12)

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

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

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 3.5.0 3.5.4 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.4.0 3.4.3 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.3.3 3.3.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.2.4 3.2.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.16 3.0.18 semver	Not specified
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XCH328	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XCM324	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XCM328	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XCM332	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRH334 24 V DC 8xFO CC	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 230 V AC 12xFO	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 230 V AC 8xFO	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 24 V DC 12xFO	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 24 V DC 8xFO	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 24V DC 2x10G 24xSFP 8xSFP	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 2x230 V AC 12xFO	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 2x230 V AC 8xFO	affected V3.3 custom	Not specified
ADP	Siemens	SCALANCE XRM334 2x230V AC 2x10G 24xSFP 8xSFP	affected V3.3 custom	Not specified
ADP	Siemens	SIDIS Prime	affected V4.0.800 custom	Not specified
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified

## References

Reference	Source	Link
<a href="https://cert-portal.siemens.com/productcert/html/ssa-089022.html">cert-portal.siemens.com/productcert/html/ssa-089022.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="#">cert-por</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-082556.html">cert-portal.siemens.com/productcert/html/ssa-082556.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="#">cert-por</a>
<a href="https://github.com/openssl/openssl/commit/7cf21a30513c9e43c4bc3836c237cf086e194af3">github.com/openssl/openssl/commit/7cf21a30513c9e43c4bc3836c237cf086e194af3</a>	openssl-security@openssl.org	<a href="#">github.c</a>
<a href="https://openssl-library.org/news/secadv/20250930.txt">openssl-library.org/news/secadv/20250930.txt</a>	openssl-security@openssl.org	<a href="#">openssl</a>
<a href="https://www.openwall.com/lists/oss-security/2025/09/30/5">www.openwall.com/lists/oss-security/2025/09/30/5</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.op</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-032379.html">cert-portal.siemens.com/productcert/html/ssa-032379.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="#">cert-por</a>
<a href="https://github.com/openssl/openssl/commit/bbf38c034cdabd0a13330abcc4855c866f53d2e0">github.com/openssl/openssl/commit/bbf38c034cdabd0a13330abcc4855c866f53d2e0</a>	openssl-security@openssl.org	<a href="#">github.c</a>
<a href="https://github.com/openssl/openssl/commit/654dc11d23468a74fc8ea4672b702dd3feb7be4b">github.com/openssl/openssl/commit/654dc11d23468a74fc8ea4672b702dd3feb7be4b</a>	openssl-security@openssl.org	<a href="#">github.c</a>
<a href="https://github.com/openssl/openssl/commit/2b4ec20e47959170422922eaff25346d362dcb35">github.com/openssl/openssl/commit/2b4ec20e47959170422922eaff25346d362dcb35</a>	openssl-security@openssl.org	<a href="#">github.c</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-485750.html">cert-portal.siemens.com/productcert/html/ssa-485750.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="#">cert-por</a>
<a href="https://github.com/openssl/openssl/commit/89e790ac431125a4849992858490bed6b225eadf">github.com/openssl/openssl/commit/89e790ac431125a4849992858490bed6b225eadf</a>	openssl-security@openssl.org	<a href="#">github.c</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Stanislav Fort (Aisle Research) (en)

**CNA:** Stanislav Fort (Aisle Research) (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](#)