Out-of-bounds read & write in RFC 3211 KEK Unwrap

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-9230
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-30 14:15:41 UTC
Updated	2026-05-12 13:17:29 UTC
Description	Issue summary: An application trying to decrypt CMS messages encrypted using password based encryption can trigger ar

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

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

EPSS: 0.000420000 probability, percentile 0.128500000 (date 2026-05-12)

Problem Types: CWE-125 | CWE-787 | CWE-125 CWE-125 Out-of-bounds Read | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/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 3.3.0 3.3.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.2.0 3.2.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.18 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1zd custom	Not specified
CNA	OpenSSL	OpenSSL	affected 1.0.2 1.0.2zm custom	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	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * 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
github.com/openssl/openssl/commit/bae259a211ada6315dc50900686daaaaaa55f482	openssl-security@openssl.org	githu
cert-portal.siemens.com/productcert/html/ssa-089022.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
github.openssl.org/openssl/extended-releases/commit/c2b96348bfa662f25f4fabf81958...	openssl-security@openssl.org	githu
lists.debian.org/debian-lts-announce/2025/10/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.
github.com/openssl/openssl/commit/9e91358f365dee6c446dcdcdb01c04d2743fd280	openssl-security@openssl.org	githu
github.openssl.org/openssl/extended-releases/commit/dfbaf161d8dafc1132dd88cd48ad...	openssl-security@openssl.org	githu
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
github.com/openssl/openssl/commit/a79c4ce559c6a3a8fd4109e9f33c1185d5bf2def	openssl-security@openssl.org	githu
openssl-library.org/news/secadv/20250930.txt	openssl-security@openssl.org	oper
github.com/openssl/openssl/commit/5965ea5dd6960f36d8b7f74f8eac67a8eb8f2b45	openssl-security@openssl.org	githu
www.openwall.com/lists/oss-security/2025/09/30/5	af854a3a-2127-422b-91ae-364da2661108	www
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
github.com/openssl/openssl/commit/b5282d677551afda7d20e9c00e09561b547b2dfd	openssl-security@openssl.org	githu
cert-portal.siemens.com/productcert/html/ssa-485750.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Discovery Credit

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Viktor Dukhovni (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**