Timing side-channel in SM2 algorithm on 64 bit ARM

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

Summary

CVE	CVE-2025-9231
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: A timing side-channel which could potentially allow remote recovery of the private key exists in the SM2 alg

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.000210000 probability, percentile 0.061010000 (date 2026-05-12)

Problem Types: CWE-385 | CWE-385 CWE-385 Covert Timing Channel

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

None

Availability

Low

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

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
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	SIMATIC CN 4100	affected V5.0 custom	Not specified

References

Reference	Source	Link
www.openwall.com/lists/oss-security/2026/05/11/11	af854a3a-2127-422b-91ae-364da2661108	www.op
cert-portal.siemens.com/productcert/html/ssa-089022.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-por
github.com/openssl/openssl/commit/cba616c26ac8e7b37de5e77762e505ba5ca51698	openssl-security@openssl.org	github.c
openssl-library.org/news/secadv/20250930.txt	openssl-security@openssl.org	openssl
www.openwall.com/lists/oss-security/2025/09/30/5	af854a3a-2127-422b-91ae-364da2661108	www.op

cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-por
github.com/openssl/openssl/commit/567f64386e43683888212226824b6a179885a0fe	openssl-security@openssl.org	github.c
github.com/openssl/openssl/commit/fc47a2ec078912b3e914fab5734535e76c4820c2	openssl-security@openssl.org	github.c
github.com/openssl/openssl/commit/eed5adc9f969d77c94f213767acbb41ff923b6f4	openssl-security@openssl.org	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Stanislav Fort (Aisle Research) (en)

CNA: Tomas Mraz (en)

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