Low-level invalid GF(2^m) parameters lead to OOB memory access

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

Summary

CVE	CVE-2024-9143
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-16 17:15:18 UTC
Updated	2026-05-12 12:17:22 UTC
Description	Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can le

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from ADP

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

EPSS: 0.008830000 probability, percentile 0.755520000 (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	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSSL	OpenSSL	affected 3.3.0 3.3.3 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.2.0 3.2.4 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.1.0 3.1.8 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.16 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1zb custom	Not specified
CNA	OpenSSL	OpenSSL	affected 1.0.2 1.0.2zl custom	Not specified
ADP	Siemens	SIDIS Prime	affected V4.0.700 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	Li
cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
github.com/openssl/openssl/commit/72ae83ad214d2eef262461365a1975707f862712	openssl-security@openssl.org	git
github.openssl.org/openssl/extended-releases/commit/8efc0cbaa8ebba8e116f7b81a876...	openssl-security@openssl.org	git
www.openwall.com/lists/oss-security/2024/10/23/1	af854a3a-2127-422b-91ae-364da2661108	ww
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
www.openwall.com/lists/oss-security/2024/10/24/1	af854a3a-2127-422b-91ae-364da2661108	ww
cert-portal.siemens.com/productcert/html/ssa-769027.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
github.openssl.org/openssl/extended-releases/commit/9d576994cec2b7aa37a91740ea7e...	openssl-security@openssl.org	git
cert-portal.siemens.com/productcert/html/ssa-277137.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	ce
www.openwall.com/lists/oss-security/2024/10/16/1	af854a3a-2127-422b-91ae-364da2661108	ww
github.com/openssl/openssl/commit/c0d3e4d32d2805f49bec30547f225bc4d092e1f4	openssl-security@openssl.org	git

github.com/openssl/openssl/commit/bc7e04d7c8d509fb78fc0e285aa948fb0da04700	openssl-security@openssl.org	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
openssl-library.org/news/secadv/20241016.txt	openssl-security@openssl.org	op
security.netapp.com/advisory/ntap-20241101-0001	af854a3a-2127-422b-91ae-364da2661108	se
github.com/openssl/openssl/commit/fdf6723362ca51bd883295efe206cb5b1cfa5154	openssl-security@openssl.org	git
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

CNA: Google OSS-Fuzz-Gen (en)

CNA: Viktor Dukhovni (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 registred 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**