NULL Pointer Dereference in PKCS12_item_decrypt_d2i_ex function

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

Summary

CVE	CVE-2025-69421
State	PUBLISHED
Assigner	openssl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-27 16:16:34 UTC
Updated	2026-05-12 13:17:26 UTC
Description	Issue summary: Processing a malformed PKCS#12 file can trigger a NULL pointer dereference in the PKCS12_item_decryp

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

Problem Types: CWE-476 | CWE-476 CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSSL	OpenSSL	affected 3.6.0 3.6.1 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.5.0 3.5.5 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.4.0 3.4.4 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.3.0 3.3.6 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 3.0.0 3.0.19 semver	Not specified
CNA	OpenSSL	OpenSSL	affected 1.1.1 1.1.1ze custom	Not specified
CNA	OpenSSL	OpenSSL	affected 1.0.2 1.0.2zn custom	Not specified
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom	Not specified

References

Reference	Source	Link
github.com/openssl/openssl/commit/3524a29271f8191b8fd8a5257eb05173982a097b	openssl-security@openssl.org	github.cor
github.com/openssl/openssl/commit/643986985cd1c21221f941129d76fe0c2785aeb3	openssl-security@openssl.org	github.cor
github.com/openssl/openssl/commit/36ecb4960872a4ce04bf6f1e1f4e78d75ec0c0c7	openssl-security@openssl.org	github.cor
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal
github.com/openssl/openssl/commit/a2dbc539f0f9cc63832709fa5aa33ad9495eb19c	openssl-security@openssl.org	github.cor
openssl-library.org/news/secadv/20260127.txt	openssl-security@openssl.org	openssl-lib
github.com/openssl/openssl/commit/4bbc8d41a72c842ce4077a8a3eccd1109aaf74bd	openssl-security@openssl.org	github.cor
CVE Program record	CVE.ORG	www.cve.(
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Luigino Camastra (Aisle Research) (en)

CNA: Luigino Camastra (Aisle Research) (en)

CNA: Luigino Camastra (Aisle Research) (en)

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