OpenSC: `sc_compacttlv_find_tag` can return out-of-bounds pointers

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-66038
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 18:16:18 UTC
Updated	2026-04-01 17:40:36 UTC
Description	OpenSC is an open source smart card tools and middleware. Prior to version 0.27.0, sc_compacttlv_find_tag searches a cc

Risk And Classification

Primary CVSS: v3.1 6.8 MEDIUM from nvd@nist.gov

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

EPSS: 0.000150000 probability, percentile 0.032870000 (date 2026-04-01)

Problem Types: CWE-126 | CWE-126 CWE-126: Buffer Over-read

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.8	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	3.9	LOW	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	3.9	LOW	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opensc Project	Opensc	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSC	OpenSC	affected < 0.27.0	Not specified

References

Reference	Source	Link	Tag
github.com/OpenSC/OpenSC/commit/6db171bcb6fd7cb3b51098fefbb3b28e44f0a79c	security-advisories@github.com	github.com	Pat
github.com/OpenSC/OpenSC/security/advisories/GHSA-72x5-fwjx-2459	security-advisories@github.com	github.com	Exp
github.com/OpenSC/OpenSC/wiki/CVE-2025-66038	security-advisories@github.com	github.com	Ver
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

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