



OpenSC: Stack-buffer-overflow WRITE in card-oberthur

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2025-66215
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 17:28:49 UTC
Description	OpenSC is an open source smart card tools and middleware. Prior to version 0.27.0, an attacker with physical access to the

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: 0.000190000 probability, percentile 0.050880000 (date 2026-04-01)

Problem Types: CWE-121 | CWE-121 CWE-121: Stack-based Buffer Overflow

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	3.8	LOW	CVSS:3.1/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	3.8	LOW	CVSS:3.1/AV:P/AC:H/PR:N/UI:R/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

Integrity

High

Availability

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/pull/3436	security-advisories@github.com	github.com	Issue
github.com/OpenSC/OpenSC/commit/efd1d479832141bcf705c2f47655ada4d5f92f5d	security-advisories@github.com	github.com	Patch
github.com/OpenSC/OpenSC/security/advisories/GHSA-q5fc-cw56-hwp2	security-advisories@github.com	github.com	Patch
github.com/OpenSC/OpenSC/wiki/CVE-2025-66215	security-advisories@github.com	github.com	Version
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

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 registered 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)