Libopensc: opensc: multiple uses of uninitialized variable

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

Summary

CVE	CVE-2025-13763
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 13:16:09 UTC
Updated	2026-04-24 14:50:56 UTC
Description	Multiple uses of uninitialized variables were found in libopensc that may lead to information disclosure or application crash.

Risk And Classification

Primary CVSS: v3.1 5.7 MEDIUM from secalert@redhat.com

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

EPSS: 0.000180000 probability, percentile 0.048360000 (date 2026-04-24)

Problem Types: CWE-457 | CWE-457 CWE-457 Use of Uninitialized Variable

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.7	MEDIUM	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	CVSS	5.7	MEDIUM	CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenSC	OpenSC	affected 0.27.0 semver	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

Reference	Source	Link
access.redhat.com/security/cve/CVE-2025-13763	secalert@redhat.com	access.redhat.com
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com
github.com/OpenSC/OpenSC/wiki/CVE-2025-13763	secalert@redhat.com	github.com
github.com/OpenSC/OpenSC/security/advisories/GHSA-2v44-fq35-98vv	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-11-27T14:28:07.219Z	Reported to Red Hat.
CNA	2026-04-23T12:09:46.867Z	Made public.

Workarounds

CNA: To mitigate this issue, avoid connecting untrusted USB devices or smart cards to systems running affected versions of Red Hat Enterprise Linux. This operational control reduces the risk of an attacker presenting a specially crafted device to exploit the uninitialized variable flaws in `libopensc`.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**