Sensitive Information Disclosure Vulnerability Caused by Trusted Domain Bypass in OPPO Wallet

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

Summary

CVE	CVE-2026-22077
State	PUBLISHED
Assigner	OPPO
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 08:16:01 UTC
Updated	2026-04-27 18:57:20 UTC
Description	OPPO Wallet APP contains a trusted domain validation flaw that allows attackers to bypass protected interface access rest

Risk And Classification

Primary CVSS: v4.0 5.6 MEDIUM from security@oppo.com

CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:A/V:D/RE:L/U:Amber

EPSS: 0.000140000 probability, percentile 0.027960000 (date 2026-04-27)

Problem Types: CWE-346 | CWE-346 CWE-346 Origin Validation Error

Version	Source	Type	Score	Severity	Vector
4.0	security@oppo.com	Secondary	5.6	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/
4.0	CNA	CVSS	5.6	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/AU:I

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Active

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:N/R:A/V:D/RE:L/U:Amber

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OPPO	OPPO Wallet APP	affected all	Not specified

References

Reference	Source	Link	Tags
security.oppo.com/en/noticeDetail	security@oppo.com	security.oppo.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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