O+ Connect Local Privilege Escalation Vulnerability

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

Summary

CVE	CVE-2026-22069
State	PUBLISHED
Assigner	OPPO
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-19 04:16:25 UTC
Updated	2026-05-19 04:16:25 UTC
Description	A local privilege escalation vulnerability exists in O+ Connect because it fails to validate the identity of the caller on the pipe

Risk And Classification

Primary CVSS: v3.1 7.3 HIGH from security@oppo.com

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

Problem Types: CWE-266 | CWE-266 CWE-266 Incorrect privilege assignment

Version	Source	Type	Score	Severity	Vector
3.1	security@oppo.com	Secondary	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:H
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
Required

Scope
Changed

Confidentiality
Low

Integrity
Low

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OPPO	O Connect	affected 16.2.0	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.