



CVE-2015-0664

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

Summary

CVE	CVE-2015-0664
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-18 23:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The IPC channel in Cisco AnyConnect Secure Mobility Client 4.0(.00051) and earlier allows local users to write to arbitrary

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:L/AC:L/Au:S/C:P/I:P/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:L/AC:L/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
Cisco AnyConnect Secure Mobility Client Command Validation Flaw Lets Local Users Execute Arbitrary Code - SecurityTracker				af854a3a-2
Cisco AnyConnect Secure Mobility Client Arbitrary Code Execution Vulnerability				af854a3a-2
CVE Program record				CVE.ORG
NVD vulnerability detail				NVD
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				