



CVE-2015-0663

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

Summary

CVE	CVE-2015-0663
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-17 02:01:49 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco AnyConnect Secure Mobility Client 4.0(.00051) and earlier does not properly implement access control for IPC mess

Risk And Classification

Primary CVSS: v2.0 6.6 from nvd@nist.gov

AV:L/AC:L/Au:N/C:N/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:N/I:C/A:C

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 Arbitrary File Write Vulnerability			af854a3a-2127-422b-91ae-364da2661108	
Cisco AnyConnect Secure Mobility Client Lets Local Users Write Arbitrary Files - SecurityTracker			af854a3a-2127-422b-91ae-364da2661108	
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.				