



CVE-2015-4211

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

Summary

CVE	CVE-2015-4211
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-24 10:59:00 UTC
Updated	2016-12-29 13:19:00 UTC
Description	Cisco AnyConnect Secure Mobility Client 3.1(60) on Windows does not properly validate pathnames, which allows local use

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	3.1(60)	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	3.1*(60*)	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	3.1*(60*)	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All

References

Reference
Cisco AnyConnect Secure Mobility Client CVE-2015-4211 Local Privilege Escalation Vulnerability
Cisco AnyConnect Client for Windows Privilege Escalation Vulnerability
Cisco AnyConnect Secure Mobility Client for Windows File/Path Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)