



CVE-2006-4982

Published on: 09/25/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:56 PM UTC

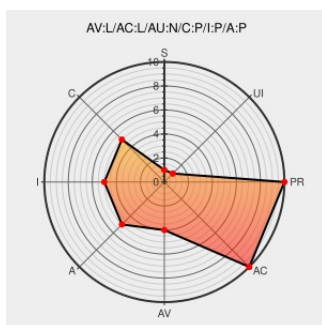
CVE-2006-4982

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Network Access Control](#) from [Cisco](#) contain the following vulnerability:

Cisco NAC maintains an exception list that does not record device properties other than MAC address, which allows physically proximate attackers to bypass control methods and join a local network by spoofing the MAC address of a different type of device, as demonstrated by using the MAC address of a disconnected printer.

CVE-2006-4982 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

[OSVDB 30978](#)

Inactive Link **Not Archived**

Page not found – Insightix Ltd.

[www.insightix.com
application/pdf](http://www.insightix.com/application/pdf)

[MISC www.insightix.com/files/pdf/Bypassing_NAC_Solutions_Whitepaper.pdf](#)

Inactive Link **Not Archived**

SecurityFocus

[www.securityfocus.com
text/html](http://www.securityfocus.com/text/html)

[BUGTRAQ 20060919 White paper release: Bypassing network access control \(NAC\) systems](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Network Access Control	All	All	All	All
Operating System	Cisco	Network Access Control	All	All	All	All
cpe:2.3:o:cisco:network_access_control:*.:.:.:.:.:.:						
cpe:2.3:o:cisco:network_access_control:*.:.:.:.:.:.:.:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→