



CVE-2008-1155

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

Summary

CVE	CVE-2008-1155
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-16 17:05:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cisco Network Admission Control (NAC) Appliance 3.5.x, 3.6.x before 3.6.4.4, 4.0.x before 4.0.6, and 4.1.x before 4.1.2 allow an attacker to execute arbitrary code with root privileges via a crafted packet.

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Network Admission Control	3.5	All	All	All

Application	Cisco	Network Admission Control	3.6	All	All	All
Application	Cisco	Network Admission Control	3.6.0	All	All	All
Application	Cisco	Network Admission Control	3.6.0.1	All	All	All
Application	Cisco	Network Admission Control	3.6.1.1	All	All	All
Application	Cisco	Network Admission Control	3.6.2.1	All	All	All
Application	Cisco	Network Admission Control	3.6.2.2	All	All	All
Application	Cisco	Network Admission Control	3.6.4.1	All	All	All
Application	Cisco	Network Admission Control	3.6.4.2	All	All	All
Application	Cisco	Network Admission Control	4.0	All	All	All
Application	Cisco	Network Admission Control	4.0.0.1	All	All	All
Application	Cisco	Network Admission Control	4.0.2.1	All	All	All
Application	Cisco	Network Admission Control	4.0.2.2	All	All	All
Application	Cisco	Network Admission Control	4.0.3.1	All	All	All
Application	Cisco	Network Admission Control	4.0.3.2	All	All	All
Application	Cisco	Network Admission Control	4.0.3.3	All	All	All
Application	Cisco	Network Admission Control	4.0.5.0	All	All	All
Application	Cisco	Network Admission Control	4.1	All	All	All
Application	Cisco	Network Admission Control	4.1.0	All	All	All
Application	Cisco	Network Admission Control	All	All	All	All
Application	Cisco	Network Admission Control	All	All	All	All
Application	Cisco	Network Admission Control	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference						S
Cisco Network Admission Control Shared Secret Information Disclosure Vulnerability						a
Cisco Network Admission Control Information Disclosure Security Issue - Advisories - Secunia						a
Cisco Network Admission Control Appliance Discloses Clean Access Server and Clean Access Manager Shared Secret - SecurityTracker						a
IBM X-Force Exchange						a
Cisco Security Advisory: Cisco Network Admission Control Shared Secret Vulnerability - Cisco Systems						a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						a
CVE Program record						C
NVD vulnerability detail						N

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](#)