CVE-2005-4332

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

Summary

CVE	CVE-2005-4332
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-17 11:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cisco Clean Access 3.5.5 and earlier on the Secure Smart Manager allows remote attackers to bypass authentication and c

Risk And Classification

Primary CVSS: v2.0 9.4 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Complete

Availability

Complete

AV:N/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	Network Admission Control Manager And Server System Software	3.3	All	All	All

Application	Cisco	Network Admission Control Manager And Server System Software	3.3.1	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.2	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.3	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.4	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.5	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.6	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.7	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.8	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.3.9	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.4	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.4.1	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.4.2	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.4.3	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.4.4	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.4.5	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.5	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.5.1	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.5.2	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.5.3	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.5.4	All	All	All
Application	Cisco	Network Admission Control Manager And Server System Software	3.5.5	All	All	All

Vendor Declared Affected Products

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

References

Reference	So
www.osvdb.org/21958	af8
Secunia - Advisories - Cisco Clean Access Manager Obsolete JSP Files Vulnerability	af8
SecurityFocus	af8
Cisco Security Response	af8
SecurityFocus	af8
Cisco Clean Access Multiple JSP Pages Access Validation Vulnerability	af8
CXSecurity - IDS	af8
www.osvdb.org/21957	af8
www.osvdb.org/21956	af8

www.osvdb.org/21956	af8
.aware - View topic - DoS possibilities in the Cisco Clean Access product line	af8
Webmail- OVH	af8
SecurityTracker.com Archives - Cisco Clean Access Lack of Authentication in Secure Smart Manager Lets Remote Users Deny Service	af8
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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