CVE-2011-0963

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

Summary

CVE	CVE-2011-0963
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-31 22:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The default configuration of the RADIUS authentication feature on the Cisco Network Admission Control (NAC) Guest Serv

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nac Guest Server	All	All	All	All

Application	Cisco	Nac Guest Server Software	1.0.0	All	All	All
Application	Cisco	Nac Guest Server Software	1.1.0	All	All	All
Application	Cisco	Nac Guest Server Software	1.1.1	All	All	All
Application	Cisco	Nac Guest Server Software	1.1.2	All	All	All
Application	Cisco	Nac Guest Server Software	1.1.3	All	All	All
Application	Cisco	Nac Guest Server Software	2.0.0	All	All	All
Application	Cisco	Nac Guest Server Software	2.0.1	All	All	All
Application	Cisco	Nac Guest Server Software	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
Cisco NAC Guest Server Configuration Error Lets Remote Users Bypass Authentication and Access the Network - SecurityTracker
Cisco Security Advisory: Cisco Network Admission Control Guest Server System Software Authentication Bypass Vulnerability - Cisco System
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.