CVE-2004-1099

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

Summary

CVE	CVE-2004-1099
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-10 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cisco Secure Access Control Server for Windows (ACS Windows) and Cisco Secure Access Control Server Solution Engin

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: NVD-CWE-Other | 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	Secure Access Control Server	3.3.1	All	All	All

Application	Cisco	Secure Access Control Server	3.3\(1\)	All	All	All
Application	Cisco	Secure Acs Solution Engine	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Cisco Secure Access Control Server Remote Authentication Bypass Vulnerability	af854a3a-2127-422b-91ae-364da266110
Cisco - Networking, Cloud, and Cybersecurity Solutions	af854a3a-2127-422b-91ae-364da266110
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da266110
P-028: Cisco Vulnerability in Cisco Secure Access Control Server (ACS) EAP-TLS Authentication	af854a3a-2127-422b-91ae-364da266110
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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