CVE-2002-0160

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

Summary

CVE	CVE-2002-0160
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-04-22 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The administration function in Cisco Secure Access Control Server (ACS) for Windows, 2.6.x and earlier and 3.x through 3.

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: NVD-CWE-Other | 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
Application	Cisco	Secure Access Control Server	2.6	All	All	All

Application	Cisco	Secure Access Control Server	2.6.2	All	All	All
Application	Cisco	Secure Access Control Server	2.6.3	All	All	All
Application	Cisco	Secure Access Control Server	2.6.4	All	All	All
Application	Cisco	Secure Access Control Server	3.0	All	All	All
Application	Cisco	Secure Access Control Server	3.0.1	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
www.osvdb.org/5352	af854a3a-2127-422b-91ae-364da2661108
Cisco - Cisco Security Advisory: Web Interface Vulnerabilities in Cisco Secure ACS for Windows	af854a3a-2127-422b-91ae-364da2661108
marc.info	af854a3a-2127-422b-91ae-364da2661108
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.