



CVE-2006-3226

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-3226
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-26 16:05:00 UTC
Updated	2018-10-18 16:46:00 UTC
Description	Cisco Secure Access Control Server (ACS) 4.x for Windows uses the client's IP address and the server's port number to gr

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Access Control Server	4.0	All	windows	All
Application	Cisco	Secure Access Control Server	4.0.1	All	windows	All
Application	Cisco	Secure Access Control Server	4.0	All	windows	All
Application	Cisco	Secure Access Control Server	4.0.1	All	windows	All

References

Reference
Cisco Secure ACS Authentication Bypass Vulnerability
Cisco Response to: Cisco Secure ACS Weak Session Management Vulnerability [Cisco Secure Access Control Server for Windows] - Cisco S
SecurityFocus
Secunia - Advisories - Cisco Secure ACS Session Management Security Issue
SecurityFocus
26825
SecurityTracker.com Archives - Cisco Secure Access Control Server Session Authentication Weakness Lets Remote Users Hijack Manageme
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
IBM X-Force Exchange
CXSecurity - IDS

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.

© [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](#)