



CVE-2005-1942

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

Summary

CVE	CVE-2005-1942
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-06-10 04:00:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	Cisco switches that support 802.1x security allow remote attackers to bypass port security and gain access to the VLAN via

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Catalyst	All	All	All	All
Hardware	Cisco	Catalyst	All	All	All	All

References

Reference	Source	Link
'Voice VLAN Access/Abuse Possible on Cisco voice-enabled,' - MARC	BUGTRAQ	marc.info
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
UltraDNS Client Redirection Service	MISC	www.fishnetsecurity.com
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO	www.cisco.com
Cisco 802.1x Voice-Enabled Interfaces Grant Anonymous Voice VLAN Access - SecurityTracker	SECTRACK	www.securitytracker.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)