



CVE-2009-2862

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

Summary

CVE	CVE-2009-2862
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-28 19:30:00 UTC
Updated	2022-06-02 17:23:00 UTC
Description	The Object Groups for Access Control Lists (ACLs) feature in Cisco IOS 12.2XNB, 12.2XNC, 12.2XND, 12.4MD, 12.4T, 12.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	ios	12.2xnb	All	All	All
Hardware	Cisco	ios	12.2xnc	All	All	All
Hardware	Cisco	ios	12.2xnd	All	All	All
Hardware	Cisco	ios	12.4md	All	All	All
Hardware	Cisco	ios	12.4t	All	All	All
Hardware	Cisco	ios	12.4xz	All	All	All
Hardware	Cisco	ios	12.4ya	All	All	All
Operating System	Cisco	ios	12.2xnb	All	All	All
Operating System	Cisco	ios	12.2xnc	All	All	All
Operating System	Cisco	ios	12.2xnd	All	All	All
Operating System	Cisco	ios	12.4md	All	All	All
Operating System	Cisco	ios	12.4t	All	All	All
Operating System	Cisco	ios	12.4xz	All	All	All
Operating System	Cisco	ios	12.4ya	All	All	All
Hardware	Cisco	ios	12.2xnb	All	All	All
Hardware	Cisco	ios	12.2xnc	All	All	All
Hardware	Cisco	ios	12.2xnd	All	All	All

Hardware	Cisco	ios	12.4md	All	All	All
Hardware	Cisco	ios	12.4t	All	All	All
Hardware	Cisco	ios	12.4xz	All	All	All
Hardware	Cisco	ios	12.4ya	All	All	All

References

Reference
tools.cisco.com/security/center/viewAlert.x
Cisco IOS Object Groups for ACLs Lets Remote Users Bypass Access Controls - SecurityTracker
Cisco Security Advisory: Cisco IOS Software Object-group Access Control List Bypass Vulnerability [Products & Services] - Cisco Systems
58338
Cisco IOS Object Group Access Control List Bypass Vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
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.