

# Cisco Security Advisory: Cisco IOS Software Object-group Access Control List Bypass Vulnerability

Advisory ID: cisco-sa-20090923-acl

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>

## Revision 1.0

For Public Release 2009 September 23 1600 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

## Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

A vulnerability exists in Cisco IOS® software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>.

**Note:** The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

[http://www.cisco.com/web/about/security/intelligence/Cisco\\_ERP\\_sep09.html](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html)

[\[Expand all sections\]](#)   [\[Collapse all sections\]](#)

## ☐ Affected Products

### ☐ Vulnerable Products

Any Cisco device configured with ACLs using the object group feature and running an affected Cisco IOS software version is affected by this vulnerability.

**Note:** The Object Groups for ACLs feature was introduced in Cisco IOS software version 12.4(20)T.

To verify whether object groups are configured in a Cisco IOS device, use the **show object-group** command in user EXEC or privileged EXEC mode. The following example displays a sample output from the **show object-group** command when object groups are configured:

```
Router# show object-group
Network object group my_host_group
```

```
host 172.18.104.123
```

```
Service object group my_allowed_services  
tcp eq www  
tcp eq 443
```

Alternatively, administrators can also use the **show running config | include ^ (permit|deny) . \*object-group** command to verify whether object groups are configured, as shown in the following example:

```
Router#show running-config | include ^ (permit|deny) .  
*object-group  
permit object-group my_allowed_services host  
10.10.1.1 host 10.20.1.1  
permit tcp any object-group my_host_group eq 22
```

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version  
Cisco Internetwork Operating System Software  
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26),  
RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2008 by cisco Systems, Inc.  
Compiled Mon 17-Mar-08 14:39 by dchih
```

*!--- output truncated*

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.4(20)T with an installed image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-
ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

*!--- output truncated*

## ☐ Products Confirmed Not Vulnerable

**Note:** The Cisco Catalyst 6500 Object Groups feature for policy-based ACLs (PBACLs) is not affected by this vulnerability.

Cisco devices that are not configured with object groups are not vulnerable.

Cisco IOS XE Software and Cisco IOS XR Software are not affected by this vulnerability.

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#)   [Close Section](#)

## ☐ Details

In Cisco IOS Software an object group can contain a single object (such as a single IP address, network, or subnet) or multiple objects (such as a combination of multiple IP addresses, networks, or subnets). In an ACL that is based on an object group, administrators can create a single access control entry (ACE) that uses an object group name instead of creating many ACEs, which each would require a different IP address. A similar object group, such as a protocol port group, can be extended to limit access to a set of applications for a user group to a server group.

**Note:** The Cisco Catalyst 6500 Object Groups feature for policy-based ACLs (PBACLs) is not affected by this vulnerability.

A vulnerability exists in Cisco IOS Software that could allow an unauthenticated attacker to bypass access control policies when the Object Groups for ACLs feature is used.

**Note:** The Object Groups for ACLs feature was introduced in Cisco IOS software version 12.4(20)T.

This vulnerability is documented in the following Cisco Bug IDs:

- [CSCsx07114](#) ( [registered](#) customers only)
- [CSCsu70214](#) ( [registered](#) customers only)
- [CSCsw47076](#) ( [registered](#) customers only)
- [CSCsv48603](#) ( [registered](#) customers only)
- [CSCsy54122](#) ( [registered](#) customers only)
- [CSCsu50252](#) ( [registered](#) customers only)

This vulnerability has been assigned Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-2862.

[Top of the section](#)   [Close Section](#)

## ☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

**Object-group Access Control List Bypass CSCsx07114, CSCsu70214, CSCsw47076, CSCsv48603, CSCsy54122, CSCsu50252**

**Calculate the environmental score of [CSCsx07114](#), [CSCsu70214](#), [CSCsw47076](#), [CSCsv48603](#), [CSCsy54122](#), [CSCsu50252](#)**

CVSS Base Score - **4.3**

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Partial	None	None

CVSS Temporal Score - **3.6**

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[Top of the section](#)   [Close Section](#)

## Impact

Successful exploitation of the vulnerability may allow an attacker to access resources that should be protected by the Cisco IOS device.

[Top of the section](#)   [Close Section](#)

## Software Versions and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column

of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases.		
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases.		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.2 based releases.		
Affected 12.3-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.3 based releases.		
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
12.4	Not Vulnerable	

12.4GC	Vulnerable; Contact your support organization per the instructions in <a href="#">Obtaining Fixed Software</a> section of this advisory	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	
12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	12.4(22)MD1	12.4(11)MD9 12.4(15)MD3 12.4(22)MD1
12.4MDA	12.4(22)MDA1	12.4(22)MDA1

12.4MR	Not Vulnerable	
12.4SW	Not Vulnerable	
12.4T	12.4(22)T2 12.4(20)T4 12.4(24)T1	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XA	Not Vulnerable	
12.4XB	Not Vulnerable	
12.4XC	Not Vulnerable	
12.4XD	Not Vulnerable	
12.4XE	Not Vulnerable	
12.4XF	Not Vulnerable	
12.4XG	Not Vulnerable	
12.4XJ	Not Vulnerable	
12.4XK	Not Vulnerable	
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	

12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Not Vulnerable	
12.4XV	Not Vulnerable	
12.4XW	Not Vulnerable	
12.4XY	Not Vulnerable	
12.4XZ	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YA	Vulnerable; first fixed in <a href="#">12.4T</a>	12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	12.4(22)YB4	12.4(22)YB4
12.4YD	12.4(22)YD1	12.4(22)YD1
12.4YE	12.4(22)YE1	12.4(22)YE1

12.4YG	Not Vulnerable	
--------	----------------	--

**Note:** No Cisco IOS-XE or Cisco IOS Software Modularity releases are affected by this vulnerability.

[Top of the section](#)   [Close Section](#)

## ☐ **Workarounds**

There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature.

[Top of the section](#)   [Close Section](#)

## ☐ **Obtaining Fixed Software**

Cisco has released free software updates that address this vulnerability. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at [http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.html](http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html), or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact [psirt@cisco.com](mailto:psirt@cisco.com) or [security-alert@cisco.com](mailto:security-alert@cisco.com) for software upgrades.

## ☐ **Customers with Service Contracts**

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

## ☐ **Customers using Third Party Support Organizations**

Customers whose Cisco products are provided or maintained through prior or existing

agreements with third-party support organizations, such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations, such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

## ☐ **Customers without Service Contracts**

Customers who purchase direct from Cisco but do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: [tac@cisco.com](mailto:tac@cisco.com)

Customers should have their product serial number available and be prepared to give the URL of this notice as evidence of entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#)   [Close Section](#)

## ☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was found during internal testing.

[Top of the section](#)   [Close Section](#)

## ☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#)   [Close Section](#)

## ☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- [cust-security-announce@cisco.com](mailto:cust-security-announce@cisco.com)
- [first-bulletins@lists.first.org](mailto:first-bulletins@lists.first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto:comp.dcom.sys.cisco@newsgate.cisco.com)

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

[Top of the section](#)   [Close Section](#)

## ☐ **Revision History**

[Top of the section](#)   [Close Section](#)

## ☐ Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html). This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#)   [Close Section](#)

### Help us help you.

☐ **Please rate this document.**

- Excellent
- Good
- Average
- Fair
- Poor

☐ **This document solved my problem.**

- Yes
- No
- Just browsing

☐ **Suggestions for improvement:**

(256 character limit)



[Home](#)[How to Buy](#)[Login](#)[Profile](#)[Feedback](#)[Site Map](#)[Help](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)