

# Cisco Security Advisory: Cable Modem Termination System Authentication Bypass

Document ID: 24562

Advisory ID: cisco-sa-20020617-cmts-md5-bypass

<http://www.cisco.com/warp/public/707/cisco-sa-20020617-cmts-md5-bypass>

## Revision 1.1

Last Updated 2002 June 19 1300 UTC (GMT)

For Public Release 2002 June 17 1900 UTC (GMT)

---

Please provide your feedback on this document.

---

**Summary**  
**Affected Products**  
**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

Two issues are described in this security advisory.

The first issue involves cable modems not manufactured by Cisco that allow a configuration file to be downloaded from an interface that is not connected to the network of the cable modem's service provider. This historical behavior allows an unauthorized configuration to be downloaded to the cable modem. Cisco is providing a feature in its own software that mitigates this vulnerability. This feature is documented as CSCdx57688.

The second issue concerns a vulnerability in Cisco IOS® Software on only the Cisco uBR7200 series and uBR7100 series Universal Broadband Routers. A defect, documented as CSCdx72740, allows the creation of a truncated, invalid configuration file that is improperly accepted as valid by the affected routers.

Both of these vulnerabilities have been exploited to steal service by reconfiguring the cable modem to remove bandwidth restrictions. Cisco is making free software upgrades available to address these issues. The most current official copy of this document is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020617-cmts-md5-bypass.shtml>.

Cisco Security Advisory: Cable Modem Termination System Authentication Bypass

# Affected Products

This section provides details on affected products.

## Vulnerable Products

Only the Cisco uBR7200 series and uBR7100 series Universal Broadband Routers are affected.

Part of the problem described in detail below is present in products produced by other manufacturers, but Cisco is providing a fix to mitigate the vulnerability.

## Products Confirmed Not Vulnerable

The Cisco uBR10000 series Universal Broadband Routers are not affected.

No other Cisco products are currently known to be affected by these vulnerabilities.

## Details

The two issues described in this document affect the proper operation of cable modem systems. One issue results from historical behavior of cable modems not manufactured by Cisco. The other issue results from a defect in Cisco IOS Software running on a cable modem termination system (CMTS) that allows a cable modem to operate with an invalid configuration.

When a cable modem in a customer premises environment (CPE) initializes, it obtains a configuration file from the service provider's network using the Trivial File Transfer Protocol (TFTP) via a coaxial cable connection to the service provider's network. Historically, cable modems from other, non-Cisco manufacturers allow the configuration information to be downloaded via the device's Ethernet interface. By running a TFTP server on a customer premises computer and setting that computer's IP address equal to the service provider's TFTP server, a different configuration file can be downloaded to such a cable modem from the customer premises network.

The industry-standard Data Over Cable Service Interface Specification (DOCSIS) for cable modem configuration information includes a Message Integrity Check (MIC) based on a Message Digest 5 (MD5) hash of the contents of the configuration. MD5 is a one-way (non-invertible) hash meaning that the input cannot be recovered from the output and the output is considered unique for a specific input. If the MIC is not correct, the cable modem registration process fails and it will not be allowed to come on line. Publicly available tools exist to create a DOCSIS-compliant configuration, including a valid MIC. The **cable shared-secret** command in Cisco IOS Software configures a password that is included in the MD5 hash that produces the MIC; without the password, it is computationally infeasible to produce the correct matching MIC, and the cable modem is prevented from registering with the service provider's network.

If the shared secret is configured identically on all of the systems within a service provider's network and TFTP spoofing is possible as shown above, then other valid configurations containing different parameters for the same service provider network can be interchanged and downloaded to a cable modem. The modem will be allowed to come on line because the shared secret is the same. In addition, while the MD5 hash is non-invertible, the shared secret to compute it can be recovered from the CMTS router configuration. It can be protected by using the **"service password-encryption"** command in Cisco IOS Software, but the command uses "mode 7" encryption, which is considered adequate only for basic protection from casual viewing.

A defect in Cisco IOS Software for the uBR7200 and uBR7100 series Universal Broadband Routers causes the MD5 test to be skipped if an MIC is not provided in the DOCSIS configuration file. A DOCSIS configuration can be modified with a hex editor to truncate the file just before the MIC and adjust other fields to produce an invalid configuration file that will be accepted by the cable modem and the CMTS. When the cable modem attempts to register, a vulnerable CMTS fails to challenge the missing MIC and allows the cable modem to come on line. Using this vulnerability, the range of possible configurations is no longer restricted to a small alternative set for the same service provider; a completely custom configuration can be generated in which all of the options can be specified. This defect is documented as CSCdx72740, and details are available to registered users of the Cisco website.

The Cisco IOS Software configuration command **cable tftp-enforce** prohibits a cable modem from registering and coming on line if there is no matching TFTP traffic through the CMTS preceding the registration attempt. This feature has been introduced via CSCdx57688 and can be viewed by registered users of the Cisco website. This new command is available on the uBR10012 router as well as the uBR7200 and uBR7100 series.

Both the **cable tftp-enforce** command feature and the fix for the MD5 authentication bypass are necessary to properly mitigate these vulnerabilities, and Cisco is making fixed software available as shown below.

Some non-Cisco cable modems may be running older versions of software that save a local copy of the configuration information and use that cached copy at registration time instead of obtaining the actual file from a TFTP server. In addition to the possibility that the cable modem is not using the proper configuration information, the cable modem's user may be mistakenly accused of attempting theft of service.

## Impact

These vulnerabilities can be exploited to commit theft of service. For example, an attacker could obtain a basic level of service from a service provider and then exploit these vulnerabilities to reconfigure the CPE cable modem to provide greater upstream and downstream data rates. Thus the attacker obtains premium service at a basic cost.

Removing limits on bandwidth could result in a denial of service or degradation of performance for other users of the same cable network segment.

## Software Versions and Fixes

The Cisco IOS Software table below provides the label of the first release within a release train that contains the fix for the vulnerability described in this notice. A release train is assumed to be vulnerable if it is included below unless it is specifically labeled "Not Vulnerable". Each row of the table describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. 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. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label). When selecting a release, keep in mind the following definitions:

- **Maintenance** – Most heavily tested, stable, and highly recommended release of a release train in any given row of the table.
- **Rebuild** – Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific defect. Although it receives less testing, it contains only the minimal changes necessary to repair the vulnerability.

- **Interim** – Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability. Interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).

**Please note that the release label shown below may not be the best release for a specific situation.** In all cases, customers should exercise caution to confirm that the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new software release. If the information is not clear, contact the Cisco TAC for assistance as shown in Obtaining Fixed Software.

More information on Cisco IOS software release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

The fixes will be available at the Software Center located at <http://www.cisco.com/public/sw-center/>.

Software installation and upgrade procedures are available at [http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](http://www.cisco.com/warp/public/130/upgrade_index.shtml).

Train	Image Description or Platform	Availability of Fixed Releases*		
<b>11.x Releases</b>		<b>Rebuild</b>	<b>Interim**</b>	<b>Maintenance</b>
11.3NA	Early Deployment release for uBR7200 series	Vulnerable, no fix available		
11.3T	Early Deployment Technology release for multiple platforms	Vulnerable, no fix available		
11.3XA	Early Deployment Technology release for cable platforms	Vulnerable, obsolete		
<b>12.0 Releases</b>		<b>Rebuild</b>	<b>Interim**</b>	<b>Maintenance</b>
12.0	General Deployment release for multiple platforms	Vulnerable, no fix available		
12.0SC	Early Deployment release for data-over-cable service providers, uBR7200 series	Vulnerable, no fix available		
12.0T	Early Deployment Technology release for multiple platforms	Vulnerable, no fix available		

12.0XR	Early Deployment Technology release for cable platforms	Vulnerable, obsolete		
<b>12.1 Releases</b>		<del>Rebuild</del>	<del>Maintenance</del>	<del>Maintenance</del>
12.1	General Deployment candidate release for multiple platforms	Vulnerable, no fix available		
12.1CX	Early Deployment Technology release for cable platforms	Vulnerable, obsolete		
12.1EC	Specific Technology Early Deployment release for uBR7200 and uBR10k series platforms	12.1(11b)EC1	12.1(11.5)EC	12.1(12)EC
12.1T	Early Deployment release for multiple platforms	2002/06/10	2002/06/14	2002/07/15
		Vulnerable, no fix available		
<b>12.2 Releases</b>		<del>Rebuild</del>	<del>Maintenance</del>	<del>Maintenance</del>
12.2	General Deployment candidate release for multiple platforms	Vulnerable, no fix available		
12.2BC	Specific Technology Early Deployment release for uBR7100, uBR7200, and uBR10k series platforms; <b>NOT VULNERABLE, but includes tftp-enforce feature</b>	12.2(8)BC1b		12.2(8)BC2
12.2T	Early Deployment Technology release for multiple platforms	2002/06/17	2002/07/15	
		Vulnerable, no fix available		
12.2XF		Vulnerable, obsolete		

Early Deployment Technology release for cable platforms
<b>Notes</b>
* All dates are estimates and subject to change.  ** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.

## Workarounds

There is no workaround for the MD5 bypass vulnerability. Customers are strongly encouraged to use the **cable tftp-enforce** command, deploy a **shared-secret** scheme and change the secret routinely, and monitor CMTS routers for evidence of tampering with bandwidth restrictions.

If the service provider has only one service profile, then the **cable qos permission enforce** command can be used to prevent cable modems from coming on line with a configuration containing any other service profile. This command is effective in all releases where it is supported.

The **no cable qos permission modem** command prevents a configuration with a new service profile from being created. This would restrict service theft to service profiles from known, pre-existing configuration files on the service provider's TFTP server, assuming the file names could be guessed and the server could be reached.

## Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. 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/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "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 agreement 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 who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their 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)

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

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

## Exploitation and Public Announcements

These vulnerabilities have been widely discussed in public and instructions for exploiting them are available on multiple websites. The Cisco PSIRT is aware of numerous incidents of theft of service by exploiting these vulnerabilities.

## 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.

## Distribution

This notice will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20020617-cmts-md5-bypass.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)

- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

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

## Revision History

Revision 1.1	<del>2002 June 19</del>	<del>Updated Workarounds section</del>
Revision 1.0	<del>2002 June 17</del>	<del>Initial public release</del>

## 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>.

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Jun 19, 2002

Document ID: 24562

---