

[NEWS] Cable Modem Termination System Authentication Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0074.html>

From: support@securiteam.com

Date: 06/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 18 Jun 2002 20:10:39 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Cable Modem Termination System Authentication Bypass

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.

DETAILS

Affected Products:

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

Securiteam: [NEWS] Cable Modem Termination System Authentication Bypass

Note that the Cisco uBR10000 series Universal Broadband Routers are not 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.

No other Cisco products are affected.

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

Securiteam: [NEWS] Cable Modem Termination System Authentication Bypass

"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:

Please see the following URL, for a complete listing for all Fixed versions:

<http://www.cisco.com/warp/public/707/cmts-MD5-bypass-pub.shtml#Software>

Securiteam: [NEWS] Cable Modem Termination System Authentication Bypass

<http://www.cisco.com/warp/public/707/cmts-MD5-bypass-pub.shtml#Software>

Obtaining Fixed Software:

Cisco is offering free software upgrades to correct this vulnerability for all affected customers. Customers with service contracts may upgrade to any software release containing the feature sets they have purchased. Customers without contracts may upgrade only within a single row of the table above, except that any available fixed software release will be provided to any customer who can use it and for whom the standard fixed software release is not yet available. Customers may only install and expect support for the feature sets they have purchased.

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 the Cisco worldwide website at <http://www.cisco.com/>. 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 assistance with the upgrade, which should be free of charge.

Customers without contracts should get their upgrades by contacting the Cisco TAC:

- * +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

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. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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 profile 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.

ADDITIONAL INFORMATION

Securiteam: [NEWS] Cable Modem Termination System Authentication Bypass

The information has been provided by <mailto:psirt@cisco.com> Cisco
Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] Malicious PHP Source Injection in phpBB (install.php)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)