

[NEWS] Security Problem Found with Cisco UBR900 Series Routers

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0018.html>

From: support@securiteam.com

Date: 01/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 4 Jan 2002 19:27:46 +0100 (CET)

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.

Security Problem Found with Cisco UBR900 Series Routers

SUMMARY

A security vulnerability in Cisco's UBR900 allows read-write access to the MIB, which leads to access to the router configuration, using any community name whatsoever.

DETAILS

Vulnerable systems:

UBR920

UBR924

UBR925

Vendor response:

Cisco PSIRT was contacted, and a local cable provider, where it was determined that this provider definitely uses the same make and model of routers. The cable company responded only to the second part of the message, which was a request for prices of business-grade cable service. The response from Cisco was as follows:

This behavior in SNMP access is due to DOCSIS 1.0 standards that specifies that by default, there is no restrictions on SNMP access to the device.

Securiteam: [NEWS] Security Problem Found with Cisco UBR900 Series Routers

Cisco has to comply with DOCSIS standards in order to produce a CableLabs certified product. Cisco has tried very hard to convince CableLabs that their approach is wrong, but have had no success. CableLabs standards provides a mechanism (via a DOCSIS configuration file) to automatically configure SNMP access list as the device attaches to the network. It is assumed (by CableLabs) that prior to this time, security is not critical since the device gets its configuration (via the DOCSIS configuration file) before anyone can do any harm.

The document is TP-OSSI-ATPv1.1-I01-011221. The specific is on 2.1.7 CM Network management Access and SNMP Co-existence (OSS-07.1), 1 Default Access. It is on page OSS-7.1 page 3 of 11.

It states "The Default Access test verifies the CM agent supports full SNMP access from an NSI side NMS and from a CPE side NMS after the CM completes registration with the basic1.cfg configuration file. The term "Default Access" implies no docsDevNmAccessTable row and no SNMPv3 configuration was supplied to the CM. Any SNMP read and any SNMP write community string can be used for this test, since compliant CMs will allow open access in the Default Access condition."

This document is available from CableLabs at <<http://www.cablemodem.com/>>
<http://www.cablemodem.com/>.

The docsis spec has explicit requirements about the implementation and it modifies what is mentioned in RFC2669. It is also explicitly stated that it overrides the RFC should any conflict arises. Cisco's implementation has been certified by CableLabs multiple times.

Once CableLabs changes its requirement, Cisco would make the modifications to its products.

Workaround:

Possible workaround would be to create a specific RW community name, and make it accessible only from a machine on the internal network, or to stop using SNMPv1 altogether, or not to use SNMP at all.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:secureks2002@yahoo.com>>
Scott.

=====

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

=====
=====

Securiteam: [NEWS] Security Problem Found with Cisco UBR900 Series Routers

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: "[EXPL] UPNP Exploit Code Released"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)