

[NEWS] Default SNMP Community in Surecom Broadband Router

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0057.html>

From: support@securiteam.com

Date: 11/18/02

From: support@securiteam.com

To: list@securiteam.com

Date: 18 Nov 2002 10:36:01 +0200

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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Default SNMP Community in Surecom Broadband Router

SUMMARY

The default router Surecom Broadband installation enables SNMP (Simple Network Management Protocol) server with default community names for read and read/write access. This would allow a remote attacker to completely compromise the remote router.

DETAILS

Vulnerable systems:

- * Surecom Broadband Router EP-4501

Both the community name public (Which allows read access to the mentioned device, providing enumeration and gathering of sensitive network information) and the community name secret (Which allows read/write access to device, thus allowing restart and change of the network settings of the broadband router) are present in the default installation of the router. The SNMP server is enabled by default from the LAN and WAN interfaces.

Impact:

This vulnerability allows LAN and internet malicious attackers to retrieve and change network settings of the router.

Securiteam: [NEWS] Default SNMP Community in Surecom Broadband Router

Possible Solutions:

Disable default SNMP implementation, or change default community names.

Vendor response:

According to the Arhont Ltd. policy, all of the found vulnerabilities and security issues will be reported to the manufacturer 7 days before releasing them to the public domains.

ADDITIONAL INFORMATION

The information has been provided by <mailto:andrei@arhont.com> Andrei Mikhailovsky.

=====

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.