

[NEWS] Samsung ADSL Modem Arbitrary File Access, Default Root Password and Root File System Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0120.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/24/05

To: list@securiteam.com

Date: 24 Mar 2005 19:11:26 +0200

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

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Samsung ADSL Modem Arbitrary File Access, Default Root Password and Root File System Access

SUMMARY

Samsung ADSL(Asymmetric Digital Subscriber Line) Modem is "a hardware based product with built in HTTPd for remote access. Samsung ADSL modems run uClinux OS".

Vulnerabilities in Samsung ADSL Modem discloses to remote user sensitive information, allows access to modem's filesystem and full access via default passwords.

DETAILS

Vulnerable Systems:

- * Different versions of Samsung ADSL modems running uClinux and Boa HTTPd
- * Depending on the implementation, other products using a combination of Boa / uClinux may be vulnerable as well.

Arbitrary File Access:

Any remote user may request any file present in the router/modem OS file

system, including files that store sensitive information. Files can be fetched unauthenticated via a GET request by pointing your browser to any of the following URLs:

- http://[SamsungModem.ip]/etc/passwd
- http://[SamsungModem.ip]/etc/hosts
- http://[SamsungModem.ip]/bin/
- http://[SamsungModem.ip]/dev/
- http://[SamsungModem.ip]/lib/
- http://[SamsungModem.ip]/tmp/
- http://[SamsungModem.ip]/var/ppp/chap-secrets
- http://[SamsungModem.ip]/bin/sh

Default Passwords:

Default user login/passwords exist in both HTTPd (http://[host]/cgi-bin/adsl.cgi) and telnet front ends:
root/root
admin/admin
user/user

Root Filesystem Access:

By telneting to the device and logging in as root/root, remote users may access the filesystem. The modem provides 256mb of ram for OS and file system operations. In this implementation there is approx 120mb free file system space which allows for the possibility for remote attackers to use the file system for malicious communication and file storage.

ADDITIONAL INFORMATION

The information has been provided by <mailto:se_cur_ity@hotmail.com> Morning Wood.

=====

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.