

[NEWS] Myvoicestream.com Security Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0052.html>

From: support@securiteam.com

Date: 01/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 13 Jan 2002 13:19:54 +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.

Myvoicestream.com Security Vulnerability

SUMMARY

A security vulnerability in myvoicestream.com allows hijacking of active sessions. This allows attackers to access sensitive information, impersonate the active account, and more.

DETAILS

Myvoicestream.com allows VoiceStream Wireless customers to manage their phones and billing accounts over SSL. Access controls to sessions are quite weak and easy to hijack; despite notifying VoiceStream in mid November 2001, security has not changed.

The two main issues that were found:

-- A browser on any host appears able to attach to a session started by another host.

-- "Log out" does not do anything substantial.

The "Log out" link at <https://myvoicestream.com> returns the user to a new login page, but the session remains valid on the server.

-- If you go to the 'update profile' page and view source, you can see the currently set password.

Securiteam: [NEWS] Myvoicestream.com Security Vulnerability

Thus: you can hijack a session, gain a potentially re-used common password, and possibly compromise other accounts with that gained information.

Considering VoiceStream has around 6 million customers, it is believed that is in fact likely that even if a malicious user were not able to determine a valid token, capturing current URLs from network traffic would be trivial in many cases. The prevalence of firewalls, application proxies and/or HTTP proxy servers like squid, and the logging generated from such elements, application would ease that ability. An even easier attack stems from the prevalence of home users with cable modems or DSL and unprotected Windows 98 or Windows 2000 hosts.

ADDITIONAL INFORMATION

The information has been provided by <mailto:trey@anvils.org> Trey Valenta and <mailto:dieman@ringworld.org> Scott Dier.

=====

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: "[TOOL] Network Sucks, connections monitor for Windows NT/2000/XP"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)