

[NEWS] www.address.com Account Hijacking Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0085.html>

From: support@securiteam.com

Date: 01/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 16 Jan 2002 20:36:17 +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.

www.address.com Account Hijacking Vulnerability

SUMMARY

<<http://www.address.com>> www.address.com has a vulnerability that allows reading the email of other users. address.com offers, among other things, free email (similar to hotmail.com).

DETAILS

The registration form used by www.address.com allows attackers to overwrite existing accounts. When it does, the password is overwritten, and the new user takes control of the account (the former user will no longer know the password).

ADDITIONAL INFORMATION

The information has been provided by Anonymous.

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

Securiteam: [NEWS] www.address.com Account Hijacking Vulnerability

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: "[NT] OpenFile Win32 API Log Overwriting/Rewriting"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)