

[NEWS] Bank of America Online Banking Insecurity

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0065.html>

From: support@securiteam.com

Date: 09/19/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NEWS] Bank of America Online Banking Insecurity

Message-Id: <20010919193850.CBB62138C1@mail.der-keiler.de>

Date: Wed, 19 Sep 2001 21:38:50 +0200 (CEST)

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.

Bank of America Online Banking Insecurity

SUMMARY

A security vulnerability was discovered in the way Bank of America handles users accessing their account information via the Internet. The vulnerability allows using of locally cached pages to access the account without the need to authenticate against the server.

Note that this attack requires the attacker to gain access to the victim's computer.

DETAILS

Users of the Bank of America Online Banking web site are vulnerable to a basic web security hole. After logging the current session out, a user can back up to a cached page

(<https://onlineid.bankofamerica.com/cgi-bin/sso.login.controller>) in their browser's history. (This is most easily reproduced in Netscape. In MSIE, the user will likely be automatically redirected to another page.)

Once on this page, the user can press the "refresh" button in their browser. This will repost the login credentials from the previous login, creating a new session, and logging the user in to the site.

Securiteam: [NEWS] Bank of America Online Banking Insecurity

Workaround:

Under Internet Explorer, it possible to not locally save encrypted pages.

- 1) Select Tools -> Internet Options
- 2) Select Advanced
- 3) Slide down until you reach the Security section
- 4) Check "Do not save encrypted pages to disk"

Vendor response:

Bank of America's Customer Service and Technical Support were notified in 8/1/2001. Both replied with canned "this will be forwarded to the appropriate parties" responses.

ADDITIONAL INFORMATION

The information has been provided by <mailto:duke33@yahoo.com> Brad Will.

=====

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] URLScan, Automatic Request Sanitization Tool from Microsoft"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)