

[NEWS] Multiple Vulnerabilities at Canada.com

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0031.html>

From: support@securiteam.com

Date: 09/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 8 Sep 2002 23:03:44 +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.

Multiple Vulnerabilities at Canada.com

SUMMARY

Multiple Vulnerabilities at Canada.com websites exist that could enable an attacker to access the e-mail account or financial portfolio of Canada.com users.

DETAILS

1. Cross Site Scripting at <http://finance.canada.com>

Canada.com's finance site, located at <http://finance.canada.com> allows users to track financial portfolios. Users enter individual stock symbols along with the quantity of shares purchased, date purchased and commission paid. The site will then track the gains and losses for the portfolio.

The finance site uses session cookies to maintain state. The cookie expires when the user either closes the browser window or logs out of the site. A cross-site scripting (XSS) vulnerability exists that would allow an attacker to access the session cookies of an authenticated user. It is important to note that because session cookies are used, the victim would need to be logged into his portfolio at the time of the attack.

The following URL provides a proof of concept for the attack. If an authenticated user were to click on the URL, their session cookies would be displayed in an alert window:

Securiteam: [NEWS] Multiple Vulnerabilities at Canada.com

[http://finance.canada.com/bin/quote/?Symbol=%22%3C/font><script>alert\(document.cookie\)</script>&x=35&y=9](http://finance.canada.com/bin/quote/?Symbol=%22%3C/font><script>alert(document.cookie)</script>&x=35&y=9)

2. Weak Session IDs at <http://finance.canada.com>

While the aforementioned vulnerability details how an attacker can steal session cookies via an XSS attack, this is not necessary if the attacker knows the username of the victim. The finance site uses the following session cookie to maintain state for a logged in user:

```
CBUSER=[username]:canada; expires=; path=/; domain=finance.canada.com
```

Simply by accessing the finance page using this cookie with an established username in the CBUSER field, it is possible to view and edit the financial portfolio set up by a legitimate user. The user does not need to be logged in at the time of the attack.

3. Cross Site Scripting at <http://mail.canada.com>

Like many web portals, Canada.com offers free e-mail accounts. Canada.com users can read and send e-mail messages via a web browser by accessing the <http://mail.canada.com> web site.

A cross-site scripting (XSS) vulnerability exists that would allow an attacker to access the session cookies of an authenticated user. It is important to note that because session cookies are used, the victim would need to be logged into his e-mail account at the time of the attack.

The following web page provides a proof of concept for the attack. If an authenticated user were to view the web page, their session cookies would be displayed in an alert window:

```
< html>
< head>
</head>
< body ONLOAD="document.forms(0).submit()">
< form method=post action="http://mail.canada.com/mail/mailbox">
< input type=hidden name="create_name"
value="<script>alert(document.cookie)</script>">
< input type=hidden name="submitted" value="true">
</form>
</body>
</html>
```

Analysis:

The XSS exploits provide a proof of concept, but could easily be modified to redirect the captured session IDs to a web server controlled by the attacker. Once the attacker obtained the session IDs they could then hijack the victim's session and access either their financial portfolio or email account. Both attacks require an element of social engineering, as the victim would need to click on the URL or view the web page. This could be accomplished by sending the URL or web page to the user via e-mail. The weak session IDs used by the finance site make it trivial for an attacker to access financial portfolios established by legitimate users.

Securiteam: [NEWS] Multiple Vulnerabilities at Canada.com

The financial portfolios are not linked to brokerages and an attacker would not therefore be able to cause financial harm to the victim. However, this does present a privacy risk due to the fact that many people use this site to track established portfolios. An attacker could therefore use this attack to gain detailed financial information.

By using the XSS attack for the mail site, an attacker could access the e-mail account of a legitimate user. Once the account is accessed the attacker could view the victim's e-mail messages or send messages from their account. This attack presents privacy and non-repudiation risks.

Detection:

All users that have established financial portfolios or e-mail accounts at Canada.com are vulnerable.

Vendor reponse:

Numerous attempts were made to contact the web site administrator(s) to inform them of the vulnerabilities but no response has yet been received.

ADDITIONAL INFORMATION

The information has been provided by <mailto:msutton@idefense.com> Michael Sutton of iDEFENSE.

=====

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: "[NT] Remotely Exploitable Buffer Overflow in PGP"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)