

[NEWS] Mozilla Cookie Stealing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0115.html>

From: support@securiteam.com

Date: 01/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 24 Jan 2002 13:34:48 +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.

Mozilla Cookie Stealing

SUMMARY

Cookies are often used to identify and authenticate users to a website. If an attacker can steal a user's cookies, then they can impersonate that user. The completeness of the impersonation and the actions the attacker can perform as that user depend on how the particular site uses the cookies.

A bug in Mozilla allows an attacker to steal the user's cookies for any given domain if the attacker can convince the user's browser to load a given URL. It does not require that active scripting is enabled in the browser, and can be done with something as simple as an image tag, allowing for hassle free use in HTML email, web based email services, etc.

DETAILS

Vulnerable systems:

Netscape versions prior to 6.2.1

Mozilla versions prior to 0.9.7

Immune systems:

Netscape version 6.2.1

Mozilla version 0.9.7

Securiteam: [NEWS] Mozilla Cookie Stealing

Background:

Cookies are the mechanism used by most websites to identify and authenticate a user. If you can steal someone's cookies, you can trick the server into thinking you are that other server. Exactly what this gains you depends on the application and how it is designed. It may gain you very little, or it may gain you a whole lot (e.g.

<<http://alive.znep.com/~marcs/passport/>> Microsoft Passport to Trouble).

For more information about cookies, see

<<http://www.cookiecentral.com/faq/>> The Unofficial Cookie FAQ.

Cookies are set with a specific hostname or a domain, so that they are only sent to that host or domain, with an exception or two. They can also be set with a specific path, or with the secure flag, which means they will only be sent if the connection is a SSL connection. Normally, this should mean that only the server that set the cookie, or others it is operating in cooperation with (e.g. in the same domain) can read it.

Mozilla has a bug that lets you bypass this protection and steal cookies for any domain. This is quite similar to bugs found in Microsoft Internet Explorer in the past (see

<<http://alive.znep.com/~marcs/security/iecookie1/>>

<http://alive.znep.com/~marcs/security/iecookie1/> and

<<http://alive.znep.com/~marcs/security/iecookie2/>>

<http://alive.znep.com/~marcs/security/iecookie2/>). As has been shown repeatedly, there are many security flaws in many Microsoft products. Sadly, they are far from being alone. There is almost certainly no web browser out there that is functional enough to browse a significant percent of current popular websites and that does not have similar security holes.

Details:

Loading a URL such as:

<<http://alive.znep.com%00www.passport.com/cgi-bin/cookies>>

<http://alive.znep.com%00www.passport.com/cgi-bin/cookies>

Will cause Mozilla to connect to the hostname specified before the "%00", but send the cookies to the server based on the entire hostname. The "%00" is the URL encoded version of the null character, used in C to terminate strings.

This exploit can be used to steal cookies with a specific path set, and can be used to steal cookies with the secure flag set, by using the specific path and SSL in the request URL. Note, however, that cookies set for a specific hostname (e.g. "www.passport.com") cannot be stolen using this method, but only cookies set for an entire domain (e.g. ".passport.com").

Example exploit:

An example exploit is available. It is in fact very straightforward:

<<http://alive.znep.com/~marcs/security/mozillacookie/demo.html>>

<http://alive.znep.com/~marcs/security/mozillacookie/demo.html>.

Securiteam: [NEWS] Mozilla Cookie Stealing

ADDITIONAL INFORMATION

The information has been provided by <mailto:marcs@znep.com> Marc Slemko.

=====

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: "[UNIX] Chuid Found to Contain Two Security Holes ('..', overwriting)"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)