

[NEWS] Mozilla Firefox Certificate Spoofing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0089.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/26/04

To: list@securiteam.com

Date: 26 Jul 2004 10:44:46 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Mozilla Firefox Certificate Spoofing

SUMMARY

Firefox has caching problem, as a result of that someone can spoof a certificate of any website and use it as his/her own. The problem is exploited using OnUnload inside <body> and redirection using HTTP-Equiv Refresh metatag, document.write() and document.close().

DETAILS

Vulnerable Systems:

* Mozilla Firefox version 0.9.1

* Mozilla Firefox version 0.9.2

Technical details:

First you direct the redirection Metatag to the website of which you want to spoof the certificate, then inside the < body> tag you add OnUnload script so you can control the output inside the web page with the spoofed certificate.

After that you say to Firefox, as soon as you unload this page close the stream, apparently the stream you close is the redirection website, you do that with document.close().

Securiteam: [NEWS] Mozilla Firefox Certificate Spoofing

Now you can write anything you want, you do that using document.write(). After writing the content of your choice you close the stream again, usually Firefox won't display your content, although if you check the source code you see it, so the last thing is to refresh the new page (do that using window.location.reload()), after that you have your domain name in the URL field, your content in the browser and the magic yellow Lock on the bottom left corner, if you pass your mouse over it you will see displayed the name of the website you spoofed the certificate, if you double click on it you will check full information of the certificate without any warning.

You don't need to have SSL in your website, it will work with HTTP.

Additionally, using this bug malicious websites can bypass content filtering using SSL properties.

Proof Of Concept Code:

```
< HTML>
< HEAD>
< TITLE>Spoofed< /TITLE>
< META HTTP-EQUIV="REFRESH" CONTENT="0;URL=https://www.example.com">
< /HEAD>
< BODY
onunload="
document.close();
document.writeln('< body onload=document.close();break;>
    < h3>It is Great to Use example\'s Cert!');
document.close();
window.location.reload();
">
< /body>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:me@cipher.org.uk>
E.Kellinis.

The original article can be found at:

http://www.cipher.org.uk/index.php?p=advisories/Certificate_Spoofing_Mozilla_FireFox_25-07-2004.advisory
http://www.cipher.org.uk/index.php?p=advisories/Certificate_Spoofing_Mozilla_FireFox_25-07-2004.advisory

=====

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

=====

Securiteam: [NEWS] Mozilla Firefox Certificate Spoofing

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.