

[Full-Disclosure] Re: Mozilla Firefox Certificate Spoofing

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-07/1410.html>

From: Stephen Samuel (samuel_at_bcgreen.com)

Date: 07/31/04

To: "E.Kellinis" <me@cipher.org.uk>
Date: Fri, 30 Jul 2004 20:16:12 -0700

Has this been posted to bugilla????

E.Kellinis wrote:

> #####
> *Application: Mozilla Firefox*
> *Vendors: <http://www.mozilla.com>*
> *Version: 0.9.1 / 0.9.2*
> *Platforms: Windows*
> *Bug: Certificate Spoofing (Phishing)*
> *Risk: High*
> *Exploitation: Remote with browser*
> *Date: 25 July 2004*
> *Author: Emmanouel Kellinis*
> *e-mail: [me@cipher\(dot\)org\(dot\)uk](mailto:me@cipher(dot)org(dot)uk)*
> *web: <http://www.cipher.org.uk>*
> *List : BugTraq(SecurityFocus)/ Full-Disclosure*
> #####
>
>
> =====
> *Product*
> =====
> *A popular Web browser,good alternative of IE and*
> *"The web browser" for linux machines,*
> *used to view pages on the World Wide Web.*
>
> ====
> *Bug*
> ====
>
> *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()*

Full-Disclosure: [Full-Disclosure] Re: Mozilla Firefox Certificate Spoofing

>
> *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 webpage with the spoofed certificate.*
>
> *After that you say to firefox, as soon as you unload this page*
> *close the stream, aparently the stream you close is*
> *the redirection website, you do that with*
> *document.close().*
>
> *Now you can write anything you want , you do that*
> *using document.write(). After writing the content of you choice*
> *you close the stream again , usually firefox wont 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 dont need to have SSL in your website ! it will work with*
> *http.*
>
> *Additional using this bug malicious websites can bypass content*
> *filtering using SSL properties.*
>
>
> =====
> *Proof Of Concept Code*
> =====
>
> < HTML>
> < HEAD>
> < TITLE>Spoofer< /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>
>
>
> =====

Full-Disclosure: [Full-Disclosure] Re: Mozilla Firefox Certificate Spoofing

> *PK:<http://www.cipher.org.uk/files/pgp/cipherorguk.public.key.txt>

> =====

--

Stephen Samuel +1(604)876-0426 samuel@bcgreen.com

<http://www.bcgreen.com/~samuel/>

Powerful committed communication. Transformation touching
the jewel within each person and bringing it to light.

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>