Abysssec Research

1) Advisory information

Title	: Firefox Plugin Parameter EnsureCachedAttrParamArrays Remote Code Execution
Version	: Firefox 3.6.4
Discovery	: http://www.abysssec.com
Vendor	: http://www.mozilla.com
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec
CVE	: CVE-2010-1214

2) Vulnerable version

Ubuntu Ubuntu Linux 9.10 sparc
Ubuntu Ubuntu Linux 9.10 powerpc
Ubuntu Ubuntu Linux 9.10 lpia
Ubuntu Ubuntu Linux 9.10 i386
Ubuntu Ubuntu Linux 9.10 amd64
Ubuntu Ubuntu Linux 9.04 sparc
Ubuntu Ubuntu Linux 9.04 powerpc
Ubuntu Ubuntu Linux 9.04 lpia
Ubuntu Ubuntu Linux 9.04 i386
Ubuntu Ubuntu Linux 9.04 amd64
Ubuntu Ubuntu Linux 8.04 LTS sparc
Ubuntu Ubuntu Linux 8.04 LTS powerpc
Ubuntu Ubuntu Linux 8.04 LTS lpia
Ubuntu Ubuntu Linux 8.04 LTS i386
Ubuntu Ubuntu Linux 8.04 LTS amd64
Ubuntu Ubuntu Linux 10.04 sparc
Ubuntu Ubuntu Linux 10.04 powerpc
Ubuntu Ubuntu Linux 10.04 i386
Ubuntu Ubuntu Linux 10.04 amd64

SuSE SUSE Linux Enterprise SDK 11 SP1
SuSE SUSE Linux Enterprise SDK 11
SuSE SUSE Linux Enterprise SDK 10 SP3
SuSE openSUSE 11.3
Slackware Linux x86_64 -current
Slackware Linux 13.1 x86_64
Slackware Linux 13.1
Slackware Linux 13.0 x86_64
Slackware Linux 13.0
Slackware Linux 12.2
Slackware Linux -current
S.u.S.E. SUSE Linux Enterprise Server 11 SP1
+ Linux kernel 2.6.5
S.u.S.E. SUSE Linux Enterprise Server 11
+ Linux kernel 2.6.5
S.u.S.E. SUSE Linux Enterprise Server 10 SP3
S.u.S.E. SUSE Linux Enterprise Desktop 11 SP1
+ Linux kernel 2.6.5
S.u.S.E. SUSE Linux Enterprise Desktop 11
S.u.S.E. SUSE Linux Enterprise Desktop 10 SP3
S.u.S.E. openSUSE 11.2
S.u.S.E. openSUSE 11.1
RedHat Fedora 13
RedHat Fedora 12
RedHat Enterprise Linux WS 4
RedHat Enterprise Linux WS 3
RedHat Enterprise Linux Optional Productivity Application 5 server
RedHat Enterprise Linux ES 4
RedHat Enterprise Linux ES 3
RedHat Enterprise Linux Desktop Workstation 5 client
RedHat Enterprise Linux Desktop 5 client
RedHat Enterprise Linux AS 4
RedHat Enterprise Linux AS 3
RedHat Enterprise Linux Desktop version 4
RedHat Enterprise Linux 5 server
RedHat Desktop 4.0
RedHat Desktop 3.0
Mozilla SeaMonkey 2.0.5
Mozilla SeaMonkey 2.0.4
Mozilla SeaMonkey 2.0.3
Mozilla SeaMonkey 2.0.2
Mozilla SeaMonkey 2.0.1
Mozilla SeaMonkey 2.0
Mozilla Firefox 3.6.4
Mozilla Firefox 3.6.3
Mozilla Firefox 3.6.2
Mozilla Firefox 3.6.2
Mozilla Firefox 3.5.10

Mozilla Firefox 3.5.9
Mozilla Firefox 3.5.8
Mozilla Firefox 3.5.7
Mozilla Firefox 3.5.6
Mozilla Firefox 3.5.5
Mozilla Firefox 3.5.4
Mozilla Firefox 3.5.3
Mozilla Firefox 3.5.2
Mozilla Firefox 3.5.1
Mozilla Firefox 3.5
Mozilla Firefox 3.6
Debian Linux 5.0 sparc
Debian Linux 5.0 s/390
Debian Linux 5.0 powerpc
Debian Linux 5.0 mipsel
Debian Linux 5.0 mips
Debian Linux 5.0 m68k
Debian Linux 5.0 ia-64
Debian Linux 5.0 ia-32
Debian Linux 5.0 hppa
Debian Linux 5.0 armel
Debian Linux 5.0 arm
Debian Linux 5.0 amd64
Debian Linux 5.0 alpha
Debian Linux 5.0
Avaya Messaging Storage Server MM3.0
Avaya Messaging Storage Server 5.2
Avaya Messaging Storage Server 5.1
Avaya Messaging Storage Server 5.0
Avaya Messaging Storage Server 4.0
Avaya Messaging Storage Server 3.1 SP1
Avaya Messaging Storage Server 3.1
Avaya Messaging Storage Server 2.0
Avaya Messaging Storage Server 1.0
Avaya Messaging Storage Server
Avaya Message Networking MN 3.1
Avaya Message Networking 5.2
Avaya Message Networking 3.1
Avaya Message Networking
Avaya IQ 5.1
Avaya IQ 5
Avaya Intuity AUDIX LX R1.1
Avaya Intuity AUDIX LX 2.0 SP2
Avaya Intuity AUDIX LX 2.0 SP1
Avaya Intuity AUDIX LX 2.0
Avaya Intuity AUDIX LX 1.0
Avaya Aura System Manager 6.0
Avaya Aura System Manager 5.2

Avaya Aura System Manager 1.0
Avaya Aura Session Manager 6.0
Avaya Aura Session Manager 5.2 SP2
Avaya Aura Session Manager 5.2 SP1
Avaya Aura Session Manager 5.2
Avaya Aura Session Manager 1.1
Avaya Aura Session Manager 1.0

3) Vulnerability information

Class

1- Code execution

Impact

An attacker can exploit this issue by tricking an unsuspecting victim into viewing a page containing malicious content. A successful exploit will result in the execution of arbitrary attacker-supplied code in the context of the user running the affected application.

Remotely Exploitable

Yes

Locally Exploitable

Yes

4) Vulnerabilities detail

In this vulnerabilty the malformed page contain a call to a plugin exist in firefox which has many vulnerable parameters. The flaw exists in xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays (void) function.

Here Is the vuleranble and patched version of the code:

UnPatch FireFox 3.6.6:

```
10822862 8d8548ffffff   lea    eax,[ebp-0B8h]
1082283d 50             push   eax
1082283e 8d45dc         lea    eax,[ebp-24h]
10822841 50             push   eax
10822842 53             push   ebx
10822843 e8b2f6ddff     call   xul!nsPluginInstanceOwner::FixUpURLS (10601efa)
```

```
10822848 6a00          push    0
1082284a 6a01          push    1
1082284c 6a01          push    1
1082284e 8d45dc        lea     eax,[ebp-24h]
10822851 50            push    eax
10822852 bfd0b79e10    mov     edi,offset xul!`string' (109eb7d0)
10822857 e804a18aff    call    xul!nsString::Trim (100cc960)
1082285c 6a00          push    0
1082285e 6a01          push    1
10822860 6a01          push    1
10822862 8d8548ffffff  lea     eax,[ebp-0B8h]
10822868 50            push    eax
10822869 e8f2a08aff    call    xul!nsString::Trim (100cc960)
1082286e 0fbfbdb0feffff movsx   edi,word ptr [ebp-150h]
10822875 33c0          xor     eax,eax
10822877 8d75dc        lea     esi,[ebp-24h]
1082287a e846e39dff    call    xul!ToNewUTF8String (10200bc5)
1082287f 0fb74b5e      movzx   ecx,word ptr [ebx+5Eh]
10822883 8b5364        mov     edx,dword ptr [ebx+64h]
10822886 03cf          add     ecx,edi
10822888 89448a04      mov     dword ptr [edx+ecx*4+4],eax ds:0023:06db7020=00000000
1082288c 33c0          xor     eax,eax
1082288e 8db548ffffff  lea     esi,[ebp-0B8h]
10822894 e82ce39dff    call    xul!ToNewUTF8String (10200bc5)
10822899 0fb74b5e      movzx   ecx,word ptr [ebx+5Eh]
1082289d 8b5368        mov     edx,dword ptr [ebx+68h]
108228a0 03cf          add     ecx,edi
108228a2 ff85b0feffff  inc     dword ptr [ebp-150h]
108228a8 89448a04      mov     dword ptr [edx+ecx*4+4],eax
108228ac 8bce          mov     ecx,esi
108228ae e81d9a92ff    call    xul!nsAString_internal::Finalize (1014c2d0)
108228b3 8d4ddc        lea     ecx,[ebp-24h]
108228b6 e8159a92ff    call    xul!nsAString_internal::Finalize (1014c2d0)
108228bb ff85acfeffff  inc     dword ptr [ebp-154h]
108228c1 0fbf85acfeffff movsx   eax,word ptr [ebp-154h]
108228c8 0fb74b60      movzx   ecx,word ptr [ebx+60h]
108228cc 3bc1          cmp     eax,ecx
108228ce 0f8ce7feffff  jl      xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays+0x746 (108227bb)
```

Patch FireFox 3.6.7:

```
1081d72e 8d8548ffffff  lea     eax,[ebp-0B8h]
1081d734 50            push    eax
1081d735 8d45dc        lea     eax,[ebp-24h]
1081d738 50            push    eax
1081d739 53            push    ebx
1081d73a e8195adfff    call    xul!nsPluginInstanceOwner::FixUpURLS (10613158)
1081d73f 33c0          xor     eax,eax
1081d741 8d75dc        lea     esi,[ebp-24h]
1081d744 e860ca9bff    call    xul!ToNewUTF8String (101da1a9)
1081d749 8b4b64        mov     ecx,dword ptr [ebx+64h]
1081d74c 8904b9        mov     dword ptr [ecx+edi*4],eax
```

```
1081d74f 33c0          xor     eax,eax
1081d751 8db548ffffff  lea     esi,[ebp-0B8h]
1081d757 e84dca9bff    call    xul!ToNewUTF8String (101da1a9)
1081d75c 8b4b68        mov     ecx,dword ptr [ebx+68h]
1081d75f 8904b9        mov     dword ptr [ecx+edi*4],eax
1081d762 8d4ddc        lea     ecx,[ebp-24h]
1081d765 47            inc     edi
1081d766 e875e98fff    call    xul!nsAString_internal::Finalize (1011c0e0)
1081d76b 8bce          mov     ecx,esi
1081d76d e86ee98fff    call    xul!nsAString_internal::Finalize (1011c0e0)
1081d772 8b85acfeffff  mov     eax,dword ptr [ebp-154h]
1081d778 038598feffff  add     eax,dword ptr [ebp-168h]
1081d77e 3b85b0feffff  cmp     eax,dword ptr [ebp-150h]
1081d784 8985acfeffff  mov     dword ptr [ebp-154h],eax
1081d78a 0f8530ffffff  jne     xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays+0x5c0 (1081d6c0)
```

xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays (void) function temporarly hold value of PARAM tags. In the vulnerable section at address 0x1082287f value of ecx register which is used as an index of acessing to memory in address 0x10822888 is filled with a 2bytes value but in the patche version it is filled with a 4byts value. and increasing the value of array cause an access violation to the memory.

To see the flaw in firefox we installed the JVM plugin on the software. For the purpose of loading the plugin to memory, we embed an applet of java to the malformed page. PARAM tag is used as an internal tag for applet tag and it is used to pass parameteres to the applet. These PARAM tags are stores as an arry temporarly. If number of tags are greater than MAX(unsigned short) , software faces an access violation in accessing the elements of the array.

An implemention of PARAM tag:

```
<APPLET code="AudioItem" width="15" height="15">
<PARAM name="snd" value="Hello.au|Welcome.au">
Java applet that plays a welcoming sound.
</APPLET>
```

In this example Hello.au, Welcome.au files are passed to the applet as snd argument.

According to the report we run Hello.au,Welcome.au command at windblg command line and here is the result:

```
10822075 xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays (void)
```

By setting a breakpoint at address xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays(void) we noticed that number of PARAM tag is used as an index for accessing element of array. So by creating

more PARAM tags the software faces Access violation exceiptopn at address 0x10822888 while accessing element of array. Here are the details of exception:

```
(1b0.4b0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=03d402a4 ebx=02a34dd0 ecx=ffff87ff edx=0561f000 esi=0012f308 edi=ffff87fa
eip=10822888 esp=0012f160 ebp=0012f32c iopl=0         nv up ei ng nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010286
xul!nsPluginInstanceOwner::EnsureCachedAttrParamArrays+0x813:
10822888 89448a04        mov     dword ptr [edx+ecx*4+4],eax ds:0023:05601000=????????
```