MOAUB

Abysssec Research

1) Advisory information

Title	: Mozilla Firefox CSS font-face Remote Code Execution Vulnerability
Version	: Firefox
Discovery	: http://www.abysssec.com
Vendor	: http://www.mozilla.com
Impact	: Ciritical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec
CVE	: CVE-2010-2752

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 ES 4
RedHat Enterprise Linux Desktop Workstation 5 client
RedHat Enterprise Linux AS 4
RedHat Enterprise Linux Desktop version 4
RedHat Enterprise Linux 5 server
RedHat Desktop 4.0
Pardus Linux 2009 0
Mozilla Thunderbird 3.0.5
Mozilla Thunderbird 3.0.4
Mozilla Thunderbird 3.0.2
Mozilla Thunderbird 3.0.1
Mozilla Thunderbird 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
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- Integer Overflow

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

This vulnerabilty exist in a structure named 'Array' in the xul! nsCSSValue class. By using the x command in windbg debugger we have searched the *!* nsCSSValue::Array expression in the vulnerable version 3.6.6 of firefox. Again searching the same expression in the patched version 3.6.7 demonstrate the followng results:

```
UnPatch FireFox 3.6.6:

0:021> x *!*nsCSSValue::Array*
101e5046 xul!nsCSSValue::Array::Array (unsigned short)
101cf2bf xul!nsCSSValue::Array::Release (void)
104bc3f4 xul!nsRefPtr<nsCSSValue::Array>::nsRefPtr<nsCSSValue::Array> (struct nsCSSValue::Array *)
10049d0c xul!nsCSSValue::Array::~Array (void)
1047f8b1 xul!nsCSSValue::Array::AddRef (void)
101e5074 xul!nsCSSValue::Array::Create (unsigned short)
104b669b xul!nsCSSValue::Array::operator== (struct nsCSSValue::Array *)
106159df xul!nsRefPtr<nsCSSValue::Array>::~nsRefPtr<nsCSSValue::Array> (void)


Patch FireFox 3.6.7:

0:022> x xul!*nsCSSValue::Array*
101ddfc2 xul!nsCSSValue::Array::Array (unsigned int)
```

```
101b4da6 xul!nsCSSValue::Array::Release (void)
104b622d xul!nsRefPtr<nsCSSValue::Array>::nsRefPtr<nsCSSValue::Array> (struct nsCSSValue::Array *)
1018d2d5 xul!nsCSSValue::Array::~Array (void)
101b8592 xul!nsCSSValue::Array::`scalar deleting destructor' (void)
10479315 xul!nsCSSValue::Array::AddRef (void)
101ddfed xul!nsCSSValue::Array::Create (unsigned int)
104b202d xul!nsCSSValue::Array::operator== (struct nsCSSValue::Array *)
1051fdfd xul!nsRefPtr<nsCSSValue::Array>::~nsRefPtr<nsCSSValue::Array> (void)
```

xul!nsCSSValue::Array::Create (unsigned short) function is responsible for creating an array that hold references to the external font resources. The input value to this function is the number of external font resources in CSS file. By comparing the vulnerable version and the patched version of the software we have noticed that in the patched version the input argument type of this function has changed to the 32bit value of unsigned int so the length of the array in the creation time will be 32bit. As it has an 32bit index.

Inorder to load a spdecial font in html by using CSS @font-face tag is used. For examle:

```
@font-face {
 font-family: Sean;
 font-style:  normal;
 font-weight: normal;
 src: url(SEAN1.eot);
font-size: 12pt;
}
```

In this example SEAN1.eot font from the current path can be used by the html page that load the CSS file. And it can be implemented like this:

<a href=”www.google.com” style=”font-family=’Sean’”>google</a>

Src field specify external font file name. This field can be set like this:

```
    src: url("type/filename.woff") format("woff")
        ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype")
         ,url("type/filename.otf") format("opentype");
```

By setting a breakpoint at address of xul!nsCSSValue::Array::Create (unsigned short), we have found that number of values set for src field is passed as an argument to this function. so by giving value larger thang MAX(unsigned short) to the src field, the software face to an access violation at address 0x100ebd86 where access to the src field. Here is the details of the error:

```
 (854.850): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0000000f ebx=01cb3000 ecx=040d6b40 edx=00670040 esi=05688ffc edi=04f44000
eip=100ebd86 esp=0012f4f0 ebp=0012f680 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010206
xul!nsCSSValue::nsCSSValue+0x46:
100ebd86 894e04          mov     dword ptr [esi+4],ecx ds:0023:05689000=????????
```

ECX register point to the address contains the values of src field. Contents of the address are shown below:

```
036cb080........o.p.e.n.t.y.p.e...l('typ.C..@... y..........mat(
036cb0b8'opentyp........o.p.e.n.t.y.p.e...tf') f.D..p... y......
036cb0f0....url('type/fi........o.p.e.n.t.y.p.e...ype').0E......
036cb128 y...........otf') forma........o.p.e.n.t.y.p.e...filena
036cb160.E...... y..........ntype')..,ur........o.p.e.n.t.y.p.e.
036cb198..mat('o.F...... y..........e/filename.o........o.p.e.n.
036cb1d0t.y.p.e...url('t@G..0... y..........ormat('opent........
036cb208o.p.e.n.t.y.p.e....otf').G..`... y...........,url('type/
036cb240........o.p.e.n.t.y.p.e...ntype'.H...... y..........me.o
036cb278tf') for........o.p.e.n.t.y.p.e...e/filePI...... y......
036cb2b0....pentype')..,........o.p.e.n.t.y.p.e...ormat(.J......
036cb2e8 y.........ype/filename........o.p.e.n.t.y.p.e....,url(
036cb320.J.. ... y.......... format('ope........o.p.e.n.t.y.p.e.
```