

Security Update Guide > Details

CVE-2016-0189 | Scripting Engine Memory Corruption Vulnerability

Security Vulnerability

Published: 05/10/2016
MITRE CVE-2016-0189

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.

The security update addresses the vulnerability by modifying how the scripting engine handles objects in memory.

On this page

- Executive Summary
- Exploitability Assessment
- Security Updates
- Mitigations
- Workarounds
- FAQ
- Acknowledgements
- Disclaimer
- Revisions

Exploitability Assessment

The following table provides an [exploitability assessment](#) for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	Yes	0 - Exploitation Detected	0 - Exploitation Detected	Not Applicable

Security Updates

To determine the support life cycle for your software version or edition, see the [Microsoft Support Lifecycle](#).

Product ▲	Platform	Article	Download	Impact	Severity	Supersedence
Internet Explorer 10	Windows Server 2012	3154070	Security Update	Remote Code Execution	Moderate	3148198
Internet Explorer 11	Windows 8.1 for 32-bit systems	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 11	Windows 8.1 for x64-based systems	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 11	Windows Server 2012 R2	3154070	Security Update	Remote Code Execution	Moderate	3148198
Internet Explorer 11	Windows RT 8.1	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 11	Windows 7 for 32-bit Systems Service Pack 1	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 11	Windows 7 for x64-based Systems Service Pack 1	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 11	Windows Server 2008 R2 for x64-based Systems Service Pack 1	3154070	Security Update	Remote Code Execution	Moderate	3148198
Internet Explorer 11	Windows 10 for 32-bit Systems	3156387	Security Update	Remote Code Execution	Critical	3147461
Internet Explorer 11	Windows 10 for x64-based Systems	3156387	Security Update	Remote Code Execution	Critical	3147461
Internet Explorer 11	Windows 10 Version 1511 for 32-bit Systems	3156421	Security Update	Remote Code Execution	Critical	3147458
Internet Explorer 11	Windows 10 Version 1511 for x64-based Systems	3156421	Security Update	Remote Code Execution	Critical	3147458
Internet Explorer 9	Windows Vista x64 Edition Service Pack 2	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 9	Windows Vista Service Pack 2	3154070	Security Update	Remote Code Execution	Critical	3148198
Internet Explorer 9	Windows Server 2008 for 32-bit Systems Service Pack 2	3154070	Security Update	Remote Code Execution	Moderate	3148198
Internet Explorer 9	Windows Server 2008 for x64-based Systems Service Pack 2	3154070	Security Update	Remote Code Execution	Moderate	3148198
Windows Server 2008 for 32-bit Systems Service Pack 2		3158991	Security Update	Remote Code Execution	Moderate	3124624
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)		3158991	Security Update	Remote Code Execution	Moderate	3124624
Windows Server 2008 for Itanium-Based Systems Service Pack 2		3158991	Security Update	Remote Code Execution	Moderate	3124624
Windows Server 2008 for x64-based Systems Service Pack 2		3158991	Security Update	Remote Code Execution	Moderate	3124624
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)		3158991	Security Update	Remote Code Execution	Moderate	3124624
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)		3155413	Security Update	Remote Code Execution	Moderate	3124625
Windows Vista Service Pack 2		3158991	Security Update	Remote Code Execution	Critical	3124624
Windows Vista x64 Edition Service Pack 2		3158991	Security Update	Remote Code Execution	Critical	3124624

Mitigations

Microsoft has not identified any [mitigating factors](#) for this vulnerability.

Workarounds

Restrict access to VBScript.dll and JScript.dll For 32-bit systems, enter the following command at an administrative command prompt:

```
takeown /f %windir%\system32\vbscript.dll
cacls %windir%\system32\vbscript.dll /E /P everyone:N
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

For 64-bit systems, enter the following command at an administrative command prompt:

```
takeown /f %windir%\syswow64\vbscript.dll
cacls %windir%\syswow64\vbscript.dll /E /P everyone:N
cacls %windir%\syswow64\jscript.dll /E /P everyone:N
```

Impact of Workaround. Websites that use VBScript or JScript may not work properly.

How to undo the workaround. For 32-bit systems, enter the following command at an administrative command prompt:

```
cacls %windir%\system32\vbscript.dll /E /R everyone
cacls %windir%\system32\jscript.dll /E /R everyone
```

For 64-bit systems, enter the following command at an administrative command prompt:

```
cacls %windir%\syswow64\vbscript.dll /E /R everyone
cacls %windir%\syswow64\jscript.dll /E /R everyone
```

FAQ

For my particular system and Internet Explorer configuration, which update addresses the vulnerabilities discussed in CVE-2016-0187 or CVE-2016-0189? CVE-2016-0187 and CVE-2016-0189 are vulnerabilities in the JScript and VBScript engines. Although the attack vector is through Internet Explorer, the vulnerabilities are addressed by the updates released in this bulletin (MS16-051) for systems running Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11. For Internet Explorer 7 and earlier, the vulnerabilities are addressed by the updates described in [MS16-053](#).

I am running Internet Explorer on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2. Does this mitigate these vulnerabilities? Yes. By default, Internet Explorer on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 runs in a restricted mode that is known as [Enhanced Security Configuration](#). Enhanced Security Configuration is a group of preconfigured settings in Internet Explorer that can reduce the likelihood of a user or administrator downloading and running specially crafted web content on a server. This is a mitigating factor for websites that you have not added to the Internet Explorer Trusted sites zone.

Can EMET help mitigate attacks that attempt to exploit these vulnerabilities? Yes. The Enhanced Mitigation Experience Toolkit (EMET) enables users to manage security mitigation technologies that help make it more difficult for attackers to exploit memory corruption vulnerabilities in a given piece of software. EMET can help mitigate attacks that attempt to exploit these vulnerabilities in Internet Explorer on systems where EMET is installed and configured to work with Internet Explorer.

For more information about EMET, see the [Enhanced Mitigation Experience Toolkit](#).

Why do I see both JScript.dll and VBScript.dll in the packages for this cumulative security update? This security update ships as a cumulative update for the JScript and VBScript scripting engines. While both engines are included in this release, the components affected by the security fixes covered by this bulletin are listed above in the section **Affected Software**.

How do I determine which versions of JScript and VBScript scripting engines are installed on my system? The JScript and VBScript scripting engines are installed with supported releases of Microsoft Windows. In addition, installing a newer version of Internet Explorer on a system can change the versions of the JScript and VBScript scripting engines that are installed.

To determine which versions of the JScript or VBScript scripting engines are installed on your system, perform the following steps:

- Open Windows Explorer.
- Navigate to the %systemroot%\system32 directory.
- For VBScript, right-click **vbscript.dll**, select **Properties**, and then click the **Details** tab.
- For JScript, right-click **jscript.dll**, select Properties, and then click the **Details** tab.

The version number is listed in the **File Version** field. If your file version starts with 5.8, for example 5.8.7600.16385, then VBScript 5.8 is installed on your system.

Once I know the versions of the JScript or VBScript scripting engine installed on my system, where do I get the update? The affected software in this bulletin apply to systems without Internet Explorer installed and to systems with Internet Explorer 7 or earlier versions installed. Customers with systems running Internet Explorer 8 or later should apply the Internet Explorer Cumulative Update ([MS16-051](#)), which also addresses the vulnerabilities discussed in this bulletin.

Acknowledgements

Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure.

See [acknowledgements](#) for more information.

Disclaimer

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

Version	Date	Description
1.0	05/10/2016	Information published.

What's new	Microsoft Store	Education	Enterprise	Developer	Company
Surface Pro X	Account profile	Microsoft in education	Azure	Microsoft Visual Studio	Careers
Surface Laptop 3	Download Center	Office for students	AppSource	Windows Dev Center	About Microsoft
Surface Pro 7	Microsoft Store support	Office 365 for schools	Automotive	Developer Network	Company news
Windows 10 apps	Returns	Deals for students & parents	Government	TechNet	Privacy at Microsoft
Office apps	Order tracking	Microsoft Azure in education	Healthcare	Microsoft developer program	Investors
	Store locations		Manufacturing	Channel 9	Diversity and inclusion
	Buy online, pick up in store		Financial services	Office Dev Center	Accessibility
	In-store events		Retail	Microsoft Garage	Security