Internet Explorer Vulnerability  
(Remote Code Execution)  
(CVE-2014-1776)
Table of Contents

Technical Summary .................................................................................................................. 3
Affected Versions ..................................................................................................................... 3
Technical Details: .................................................................................................................. 3
Recommendations .................................................................................................................. 3
Patching .................................................................................................................................. 3
Workaround ........................................................................................................................... 3
Monitoring/Detection ............................................................................................................. 7
References .............................................................................................................................. 9
Revisions ................................................................................................................................. 10
Technical Summary
FireEye Research Labs identified a new Internet Explorer (IE) zero-day exploit used in targeted attacks. The vulnerability affects IE6 through IE11, but the attack is targeting IE9 through IE11. This zero-day bypasses both ASLR and DEP. Microsoft has assigned CVE-2014-1776 to the vulnerability and released security advisory to track this issue.

The vulnerability exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website.

Affected Versions
- Internet Explorer 6 – Internet Explorer 11
- A full reference can be found here

Technical Details:
The exploit leverages a previously unknown use-after-free vulnerability, and uses a well-known Flash exploitation technique to achieve arbitrary memory access and bypass Windows’ ASLR and DEP protections. This affects the EOL Windows XP operating system and it is unknown at this time if Microsoft will be issuing patches for Windows XP.

Recommendations

Strategic
This vulnerability and others targeting Windows XP are likely to increase in the near future as organization’s struggle to eliminate Windows XP. Windows XP is no longer supported by Microsoft and as a result vulnerabilities in Windows XP and other built-in applications will not receive security patches. We highly recommend organizations that are still in the process of migrating off of XP to utilize Microsoft EMET with the Maximum security policy to mitigate this attack and future attacks.

Patching
As of April 28th, 2014, Microsoft has not released a patch but has recommended a workaround located in their advisory. Note that EMET can actually mitigate this even on a vulnerable version of windows XP that is no longer supported by Microsoft.

Workaround

- **Block access to Internet Explorer Except to Trusted Sites** – Implement content filtering controls to block access to untrusted sites. Consumer grade content filtering product vendors are releasing signatures to block this attack.
- **Consider using alternative browsers as an interim solution** – Firefox and Chrome are not affected.
- **Disabling the flash plugin in IE** – This will prevent current exploits from functioning but this may break browser functionality.
- **Deploy the Enhanced Mitigation Experience Toolkit 4.1**

The Enhanced Mitigation Experience Toolkit (EMET) helps mitigate the exploitation of this vulnerability by adding additional protection layers that make the vulnerability harder to exploit. EMET 4.1 is officially supported by Microsoft. At this time, EMET is only available in the English language. For more information, see Microsoft Knowledge Base Article 2458544.
**Note** EMET 3.0 does not mitigate this issue.
For more information about configuring EMET, see the EMET User’s Guide:

- On 32-bit systems the EMET User's Guide is located in C:\Program Files\EMET\EMET User's Guide.pdf
- On 64-bit systems the EMET User's Guide is located in C:\Program Files (x86)\EMET\EMET User's Guide.pdf

**Configure EMET 4.1 for Internet Explorer**
EMET 4.1, in the recommended configuration, is automatically configured to help protect Internet Explorer. No additional steps are required.

**Configure EMET for Internet Explorer using Group Policy**
EMET can be configured using Group Policy. For information about configuring EMET using Group Policy, see the EMET User's Guide:

- On 32-bit systems the EMET User's Guide is located in C:\Program Files\EMET\EMET User's Guide.pdf
- On 64-bit systems the EMET User's Guide is located in C:\Program Files (x86)\EMET\EMET User's Guide.pdf

- **Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones**

You can help protect against exploitation of this vulnerability by changing your settings for the Internet security zone to block ActiveX controls and Active Scripting. You can do this by setting your browser security to High.

To raise the browsing security level in Internet Explorer, perform the following steps:

1. On the Internet Explorer **Tools** menu, click **Internet Options**.
2. In the **Internet Options** dialog box, click the **Security** tab, and then click **Internet**.
3. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High.
4. Click **Local intranet**.
5. Under **Security level for this zone**, move the slider to **High**. This sets the security level for all websites you visit to High.
6. Click **OK** to accept the changes and return to Internet Explorer.

**Note** If no slider is visible, click **Default Level**, and then move the slider to **High**.

**Note** Setting the level to High may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the security setting set to High.

**Impact of workaround.** There are side effects to blocking ActiveX Controls and Active Scripting. Many websites that are on the Internet or on an intranet use ActiveX or Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX Controls to provide menus, ordering forms, or even account statements. Blocking ActiveX Controls or Active Scripting is a global setting that affects all Internet and intranet sites. If you do not want to block ActiveX Controls or Active Scripting for such sites, use the steps outlined in "Add sites that you trust to the Internet Explorer Trusted sites zone".
Add sites that you trust to the Internet Explorer Trusted sites zone

After you set Internet Explorer to block ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect yourself from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.

To do this, perform the following steps:

7. In Internet Explorer, click Tools, click Internet Options, and then click the Security tab.
8. In the Select a web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
9. If you want to add sites that do not require an encrypted channel, click to clear the Require server verification (https:) for all sites in this zone check box.
10. In the Add this website to the zone box, type the URL of a site that you trust, and then click Add.
11. Repeat these steps for each site that you want to add to the zone.
12. Click OK two times to accept the changes and return to Internet Explorer.

Note Add any sites that you trust not to take malicious action on your system. Two in particular that you may want to add are *.windowsupdate.microsoft.com and *.update.microsoft.com. These are the sites that will host the update, and it requires an ActiveX Control to install the update.

Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone

You can help protect against exploitation of this vulnerability by changing your settings to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone. To do this, perform the following steps:

1. In Internet Explorer, click Internet Options on the Tools menu.
2. Click the Security tab.
3. Click Internet, and then click Custom Level.
4. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
5. Click Local intranet, and then click Custom Level.
6. Under Settings, in the Scripting section, under Active Scripting, click Prompt or Disable, and then click OK.
7. Click OK two times to return to Internet Explorer.

Note Disabling Active Scripting in the Internet and Local intranet security zones may cause some websites to work incorrectly. If you have difficulty using a website after you change this setting, and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly.

Impact of workaround. There are side effects to prompting before running Active Scripting. Many websites that are on the Internet or on an intranet use Active Scripting to provide additional functionality. For example, an online e-commerce site or banking site may use Active Scripting to provide menus, ordering forms, or even account statements. Prompting before running Active Scripting is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click Yes to run Active Scripting. If you do not want to be prompted for all these sites, use the steps outlined in "Add sites that
you trust to the Internet Explorer Trusted sites zone”.

Add sites that you trust to the Internet Explorer Trusted sites zone
After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to the Internet Explorer Trusted sites zone. This will allow you to continue to use trusted websites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.
To do this, perform the following steps:

8. In Internet Explorer, click Tools, click Internet Options, and then click the Security tab.
9. In the Select a web content zone to specify its current security settings box, click Trusted Sites, and then click Sites.
10. If you want to add sites that do not require an encrypted channel, click to clear the Require server verification (https:) for all sites in this zone check box.
11. In the Add this website to the zone box, type the URL of a site that you trust, and then click Add.
12. Repeat these steps for each site that you want to add to the zone.
13. Click OK two times to accept the changes and return to Internet Explorer.

Note Add any sites that you trust not to take malicious action on your system. Two in particular that you may want to add are *.windowsupdate.microsoft.com and *.update.microsoft.com. These are the sites that will host the update, and it requires an ActiveX Control to install the update.

- Unregister VGX.DLL
  1. Click Start, click Run, type "%SystemRoot%\System32\regsvr32.exe" -u "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll", and then click OK.
  2. A dialog box appears to confirm that the un-registration process has succeeded. Click OK to close the dialog box.

Impact of Workaround: Applications that render VML will no longer do so once vgx.dll has been unregistered.
When a security update is available to address this issue, you should re-register vgx.dll after installing the security update. To re-register vgx.dll follow these steps:

3. Click Start, click Run, type "%SystemRoot%\System32\regsvr32.exe" "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll", and then click OK.
4. A dialog box appears to confirm that the registration process has succeeded. Click OK to close the dialog box.

- Modify the Access Control List on VGX.DLL to be more restrictive
To modify the Access Control List (ACL) on vgx.dll to be more restrictive, follow these steps:

1. Click Start, click Run, type “cmd” (without the quotation marks), and then click OK.
2. Type the following command at a command prompt make a note of the current ACL’s that are on the file (including inheritance settings) for future reference to undo this modification:

   cacls "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll"

3. Type the following command at a command prompt to deny the 'everyone' group access to this
Internet Explorer Vulnerability (Remote Code Execution (CVE-2014-1776))

Revision: 0.1

Impact of Workaround: Applications and Web sites that render VML may no longer display or function correctly.

How to undo this workaround. Before any security updates that fix this issue can be installed, this workaround must be reverted to the previous ACL configuration for vgx.dll. To revert to the previous vgx.dll ACL’s follow these steps:

5. Click Start, click Run, type “cmd” (without the quotation marks), and then click OK.
6. To revert to the previous ACL configuration for vgx.dll, type the following command and replace the ACL on vgx.dll with the ACL’s it previously had, which were recorded in step 2 of this workaround The command line to do so will vary depending on your environment:

   echo y|cacls “%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll” /g original ACL’s

7. Close Internet Explorer, and reopen it for the changes to take effect.

Note If this workaround is applied, software that redistributes vgx.dll may fail to install. Before this software can be installed, this workaround must be reverted to the previous ACL configuration for vgx.dll.

• Enable Enhanced Protected Mode For Internet Explorer 11 and Enable 64-bit Processes for Enhanced Protected Mode

Internet Explorer 11 users can help protect against exploitation of this vulnerability by changing the Advanced Security settings for Internet Explorer. You can do this by enabling Enhanced Protected Mode (EPM) settings in your browser. This security setting will protect users of Internet Explorer 11 on Windows 7 for x64-based systems, and all Windows 8 and Windows 8.1 clients.

To enable EPM in Internet Explorer, perform the following steps:

1. On the Internet Explorer Tools menu, click Internet Options.
2. In the Internet Options dialog box, click the Advanced tab, and then scroll down to the Security section of the settings list.
3. Ensure the checkboxes next to Enable Enhanced Protected Mode and Enable 64-bit processes for Enhanced Protected Mode (for 64-bit systems) are selected.
4. Click OK to accept the changes and return to Internet Explorer.
5. Restart your system.

Monitoring/Detection

The following vendors have released signatures for detecting the attack at the time of writing:

• Symantec
  o Bloodhound.Exploit.552
• Microsoft EMET -Microsoft EMET can detect and mitigate the attack. Organizations implementing detailed event logging for EMET will have visibility into this attack.
• FireEye – FireEye has disclosed a signature that will be implemented for all products by 4/29/2014
- Palo Alto Networks – A signature (36435) has been released to detect and mitigate by default.
- Mcafee – Currently developing signatures.
References

# Revisions

<table>
<thead>
<tr>
<th>Release Version:</th>
<th>1.0 – Initial Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td>4/28/2014</td>
</tr>
<tr>
<td>Summary of Changes:</td>
<td>Initial release</td>
</tr>
</tbody>
</table>