JAN
21
0

Unpatched Internet Explorer Zero Day exploited in the wild

Posted by Vidita V Koushik

Microsoft has released an emergency advisory for an **unpatched zero-day vulnerability** in **Internet Explorer**. Microsoft is also aware of limited targeted **attacks in the wild**. This vulnerability was discovered by Clement Lecigne of Google's Threat Analysis Group.

The fix for this zero-day would be released as a part of the next Patch Tuesday updates. And until then, the vulnerable Internet Explorers would be open to attack. Microsoft has also added that, this vulnerability can be exploited when any website utilizing **jscript** is accessed using a vulnerable IE browser.

Update:
360 security experts have attributed the active exploitation of **CVE-2020-0674** to an APT group named DarkHotel (APT-C-06). DarkHotel APT is known to have an East Asian background and has been operating since at least 2007. Their main targets include government organizations and enterprises.

CVE-2020-0674 : The scripting engine memory corruption vulnerability

According to Microsoft, **CVE-2020-0674** is a remote code execution vulnerability in Internet Explorer due to improper handling of objects in memory by the scripting engine. Successful exploitation could allow an attacker to **execute arbitrary code** in the context of the current user. If the targeted user has administrative privileges, then the attacker is granted administrator rights after exploitation, which he can use to install programs; view, change or delete data; or create new accounts with full user rights and completely **compromise the target system**.

Any application which supports embedding Internet Explorer or its scripting engine component would be a potential attack vector for this vulnerability. An attacker can host a **malicious website** designed to exploit the underlying vulnerability in Internet Explorer or craft **HTML documents, PDF files, Microsoft Office documents,** or any other documents which support embedded Internet Explorer scripting engine content. A user can be tricked into visiting the malicious website by clicking on links or convinced to open crafted files delivered through **spearphishing emails**.

Impact

An attacker can **remotely execute arbitrary code** on the target system and take control of the entire system in some cases.

Affected Systems

Internet Explorer 11	Internet Explorer 10	Internet Explorer 9
Windows 10 for 32/64-bit Systems Windows 10 Version 1803 for 32/64-bit Systems Windows 10 Version 1809 for 32/64-bit Systems Windows 10 Version 1909 for 32/64-bit Systems Windows 10 Version 1709 for 32/64-bit Systems Windows 10 Version 1903 for 32/64-bit Systems Windows 10 Version 1607 for 32/64-bit Systems Windows 7 Service Pack 1 for 32/64-bit Systems Windows 8.1 for 32/64-bit systems Windows RT 8.1 Windows Server 2008 R2 SP1 for x64-based Systems Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Windows Server 2012	Windows Server 2008 for 32/64 bit Systems SP 2

Mitigation/Solution

We are not aware of any updates released by Microsoft to fix the vulnerability. However, Microsoft has provided a workaround which is recommended to be applied by users who are at elevated risk. Implementation of this workaround could result in reduced functionality for components or features that rely on jscript.dll.

Restrict access to JScript.dll

For 32-bit systems, enter the following command at an administrative command prompt:

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

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

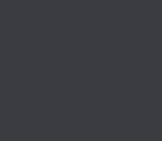
```
takeown /f %windir%\syswow64\jscript.dll
cacls %windir%\syswow64\jscript.dll /E /P everyone:N
takeown /f %windir%\system32\jscript.dll
cacls %windir%\system32\jscript.dll /E /P everyone:N
```

NOTE: This workaround must be reverted before installing any future updates.

Update:
0patch has provided a micropatch for CVE-2020-0674 which acts a 'kill switch for vulnerable jscript.dll'. This patch is also known to avoid the negative side effects of Microsoft's workaround. When Microsoft releases a patch for this vulnerability, it will be superior to the enabled micropatch.

We will continue to monitor this vulnerability and update as and when a fix is available. It is suggested for users to be extremely cautious before opening any suspicious links or documents which might trigger the vulnerability

Summary



Article Name	Unpatched Internet Explorer Zero Day exploited in the wild
Author	Vidita V Koushik
Publisher Name	SecPod Technologies
Publisher Logo	secpod Expose the Unknown

Endpoint Security, Security Research
Internet Explorer, Internet Explorer Zero-Day, microsoft, Microsoft Vulnerabilities, Remote Code Execution

← Critical Windows CryptoAPI Vulnerability demands prompt action

Critical Security Updates released for Cisco FMC →

Leave a Reply

Your email address will not be published. Required fields are marked *

Start typing...

Name *

Email *

Website

POST COMMENT

Recent Posts

From Never Wanted to be in Technology to Building Products for SecPod

Measures To Secure Oracle Solaris OS

Beware: Critical Wormable SMBv3 Flaw in Windows Systems

New class of attacks discovered in Intel Processors

Patch Tuesday: Microsoft Security Bulletin Summary for March 2020

Categories

CEO Speak

Computer Engineering

Culture

Endpoint Security

Infographics

SCAP Feed

SecPod

Security Research