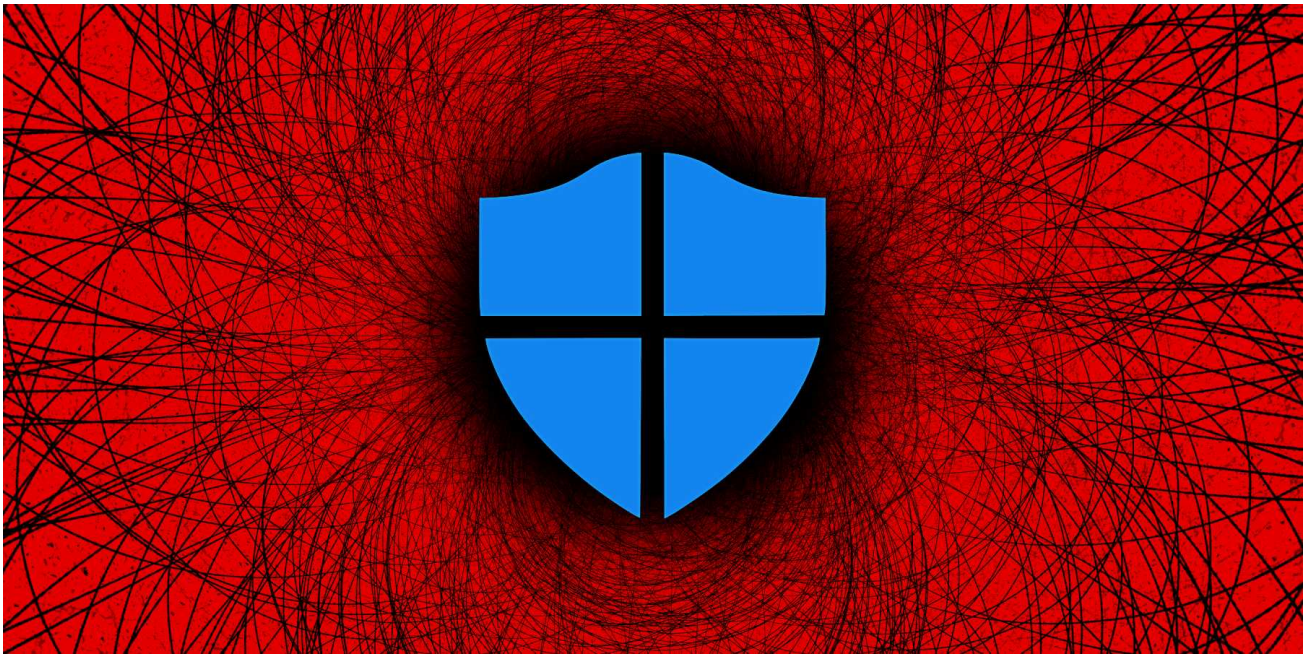
Microsoft shares temp fix for ongoing Office 365 zero-day attacks

bleepingcomputer.com/news/security/microsoft-shares-temp-fix-for-ongoing-office-365-zero-day-attacks/

Ionut Ilascu

By
Ionut Ilascu

- September 7, 2021
- 03:36 PM
- 3



Microsoft today shared mitigation for a remote code execution vulnerability in Windows that is being exploited in targeted attacks against Office 365 and Office 2019 on Windows 10.

The flaw is in MSHTML, the browser rendering engine that is also used by Microsoft Office documents.

Ongoing attacks against Office 365

Identified as CVE-2021-40444, the security issue affects Windows Server 2008 through 2019 and Windows 8.1 through 10 and has a severity level of 8.8 out of the maximum 10.

Microsoft is aware of targeted attacks that try to exploit the vulnerability by sending specially-crafted Microsoft Office documents to potential victims, the company says in an advisory today.

“An attacker could craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. The attacker would then have to convince the user to open the malicious document” - Microsoft

However, the attack is thwarted if Microsoft Office runs with the default configuration, where documents from the web are opened in Protected View mode or Application Guard for Office 365.

Protected View is a read-only mode that has most of the editing functions disabled, while Application Guard isolates untrusted documents, denying them access to corporate resources, the intranet, or other files on the system.

Systems with active Microsoft’s Defender Antivirus and Defender for Endpoint (build 1.349.22.0 and above) benefit from protection against attempts to exploit CVE-2021-40444.

Microsoft's enterprise security platform will display alerts about this attack as "Suspicious Cpl File Execution."

Researchers from multiple cybersecurity companies are credited for finding and reporting the vulnerability: Haifei Li of EXPMON, Dhanesh Kizhakkinan, Bryce Abdo, and Genwei Jiang - all three of Mandiant, and Rick Cole of Microsoft Security Intelligence.

In a tweet today, EXPMON (exploit monitor) says that they found the vulnerability after detecting a “highly sophisticated zero-day attack” aimed at Microsoft Office users.

source: EXPMON

EXPMON researchers reproduced the attack on the latest Office 2019 / Office 365 on Windows 10.

In a reply to BleepingComputer, Haifei Li of EXPMON said that the attackers used a .DOCX file. Upon opening it, the document loaded the Internet Explorer engine to render a remote web page from the threat actor.

Malware is then downloaded by using a specific ActiveX control in the web page. Executing the threat is done using "a trick called 'Cpl File Execution'," referenced in Microsoft's advisory.

The researcher told us that the attack method is 100% reliable, which makes it very dangerous. He reported the vulnerability to Microsoft early Sunday morning.

Workaround for CVE-2021-40444 zero-day attacks

As there is no security update available at this time, Microsoft has provided the following workaround - disable the installation of all ActiveX controls in Internet Explorer.

A Windows registry update ensures that ActiveX is rendered inactive for all sites, while already available ActiveX controls will keep functioning.

Users should save the file below with the .REG extension and execute it to apply it to the Policy hive. After a system reboot, the new configuration should be applied.

As updates are not available yet for the CVE-2021-40444, they have released the following workaround that prevents ActiveX controls from running in Internet Explorer and applications that embed the browser.

To disable ActiveX controls, please follow these steps:

1. Open Notepad and paste the following text into a text file. Then save the file as **disable-activex.reg**. Make sure you have the displaying of file extensions enabled to properly create the Registry file.

   Alternatively, you can download the registry file from here.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0]
"1001"=dword:00000003
"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\1]
"1001"=dword:00000003
"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\2]
"1001"=dword:00000003
"1004"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3]
"1001"=dword:00000003
"1004"=dword:00000003
```

2. Find the newly created **disable-activex.reg** and double-click on it. When a UAC prompt is displayed, click on the **Yes** button to import the Registry entries.
3. Reboot your computer to apply the new configuration.

Once you reboot your computer, ActiveX controls will be disabled in Internet Explorer.

When Microsoft provides an official security update for this vulnerability, you can remove this temporary Registry fix by manually deleting the created Registry keys.

Alternatively, you can utilize this reg file to automatically delete the entries.

Update [September 7, 2021, 16:46 EST]: Added comment received after publication from Haifei Li of EXPMON, one of the researchers that reported the vulnerability to Microsoft.

Related Articles:

Magniber ransomware gang now exploits Internet Explorer flaws in attacks

Microsoft finds severe bugs in Android apps from large mobile providers

Get more from Microsoft Office with this training suite deal

Zyxel fixes firewall flaws that could lead to hacked networks

Critical F5 BIG-IP vulnerability exploited to wipe devices

- CVE-2021-40444
- Internet Explorer
- Microsoft
- Microsoft Office
- Mitigation
- Remote Code Execution
- Vulnerability
- Workaround

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

stevansky - 8 months ago

I thought MS had phased out IE in favor of Edge? I no longer have IE on my computers, and Edge is just taking up space. I prefer Chrome based browsers myself. Edge is of course, but I think they're somewhat behind the curve compared to others.

- 
  doriel - 8 months ago
  -
  -
  "I thought MS had phased out IE in favor of Edge?"
  They had, but in older systems like Windows Server 2008, IE is still present,
- 
  askmorequestions - 8 months ago
  -
  -
  Is there a typo? It looks like the bottom 4 should be HKLM\SOFTWARE\WOW6432Node\Policies instead of HKLM\SOFTWARE\Policies\WOW6432Node .

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: