QUANTUM cybersecurity SKILLS

Early Security Alert

Proactively helping to detect threats, attacks, and vulnerabilities, identifying malicious activities to quickly mitigate them.

Severity:	**High**	**Date**:	Sept. 8 2021
Impact:	**High**	**Type**:	**Remote code execution vulnerability**
Threat/Attack vector:	**Network**		

Microsoft MSHTML Remote Code Execution Vulnerability CVE-2021-40444

Description.

Microsoft has released mitigations and workarounds to address a remote code execution vulnerability (CVE-2021-40444) in Microsoft Windows. Exploitation of this vulnerability may allow a remote attacker to take control of an affected system. According to Expmon, **the vulnerability impacts the latest versions of both the offline and online instances of Microsoft Office.**
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**. This vulnerability has been detected in exploits in the wild.

Current Exploit Price

The structure of the vulnerability defines a possible price range of **USD $25k-$100k** at the moment.
(Estimation calculated on 08/08/2021).

Affected products.

Multiple versions of Windows 7, 8.1 & 10; Windows Server 2004, 2008, 2012, 2016, 2019 & 2022. Detailed **HERE**.

Recommendations.

Disabling the installation of all ActiveX controls in Internet Explorer mitigates this attack. This can be accomplished for all sites by updating the registry. Previously-installed ActiveX controls will continue to run, but do not expose this vulnerability.
Warning. If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

1. To disable ActiveX controls on an individual system:

To disable installing ActiveX controls in Internet Explorer in all zones, paste the following into a text file and save it with the .reg file extension:

```
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. Double-click the .reg file to apply it to your Policy hive.
3. Reboot the system to ensure the new configuration is applied.

Impact of workaround. This sets the URLACTION_DOWNLOAD_SIGNED_ACTIVEX (0x1001) and URLACTION_DOWNLOAD_UNSIGNED_ACTIVEX (0x1004) to DISABLED (3) for all internet zones for 64-bit and 32-bit processes. New ActiveX controls will not be installed. Previously-installed ActiveX controls will continue to run. **How to undo the workaround.** Delete the registry keys that were added in implementing this workaround.

References.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444
https://us-cert.cisa.gov/ncas/current-activity/2021/09/07/microsoft-releases-mitigations-and-workarounds-cve-2021-40444

Take a full advantage of your services,
generate valuable business risk indicators to the board,
because being ready and prepared to face the next attack
it's totally possible and it is our duty!

QUANTUM cybersecurity SKILLS

Contact us, and let us help:
csirt@QuantumCybersecuritySkills.com
@SOCoptimization
www.QuantumCybersecuritySkills.com