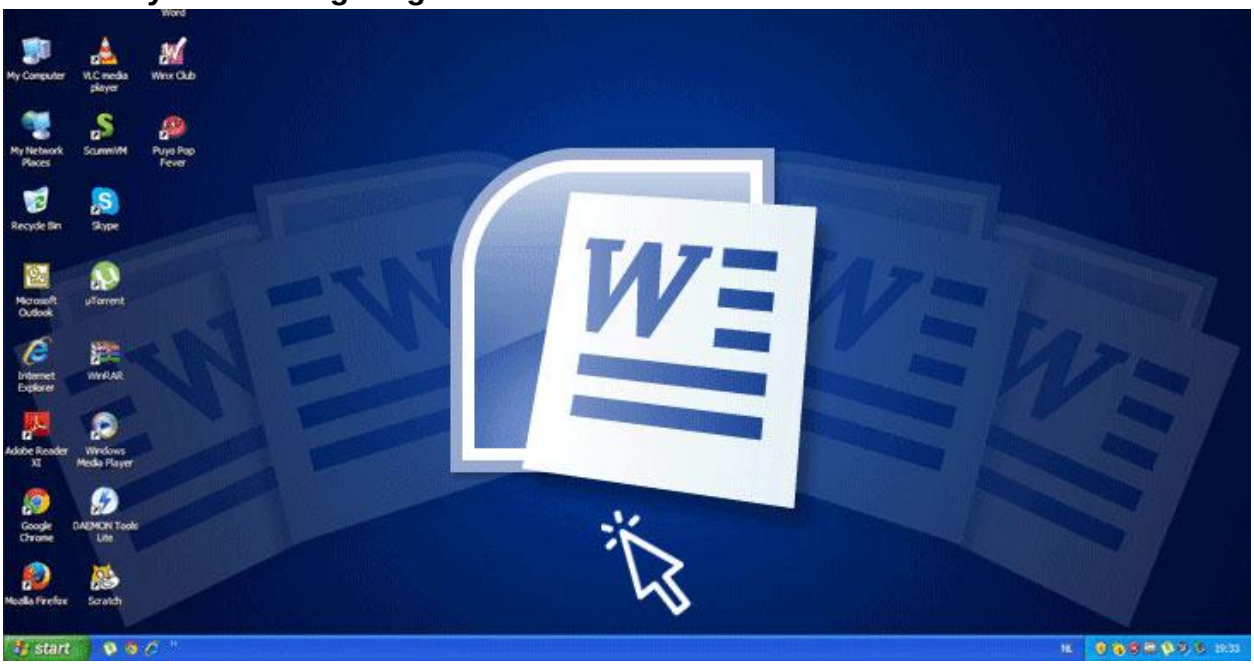
H E A D Q U A R T E R S
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

New 0-Day Attack Targeting Windows Users With Microsoft Office Documents



Microsoft on Tuesday warned of an actively exploited zero-day flaw impacting Internet Explorer that's being used to hijack vulnerable Windows systems by leveraging weaponized Office documents.

Tracked as CVE-2021-40444 (CVSS score: 8.8), the remote code execution flaw is rooted in MSHTML (aka Trident), a proprietary browser engine for the now-discontinued Internet Explorer and which is used in Office to render web content inside Word, Excel, and PowerPoint documents.

"Microsoft is investigating reports of a remote code execution vulnerability in MSHTML that affects Microsoft Windows. Microsoft is aware of targeted attacks that attempt to exploit this vulnerability by using specially-crafted Microsoft Office documents," the company said.

"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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights," it added.

The Windows maker credited researchers from EXPMON and Mandiant for reporting the flaw, although the company did not disclose additional specifics about the nature of the attacks, the identity of the adversaries exploiting this zero-day, or their targets in light of real-world attacks.

EXPMON, in a tweet, noted it found the vulnerability after detecting a "highly sophisticated zero-day attack" aimed at Microsoft Office users, adding it passed on its findings to Microsoft on Sunday. "The exploit uses logical flaws so the exploitation is perfectly reliable (& dangerous)," EXPMON researchers said.

However, it's worth pointing out that the current attack can be suppressed if Microsoft Office is run with default configurations, wherein documents downloaded from the web are opened in Protected View or Application Guard for Office, which is designed to prevent untrusted files from accessing trusted resources in the compromised system.

Microsoft, upon completion of the investigation, is expected to either release a security update as part of its Patch Tuesday monthly release cycle or issue an out-of-band patch "depending on customer needs." In the interim, the Windows maker is urging users and organizations to disable all ActiveX controls in Internet Explorer to mitigate any potential attack.

Recommendation(s)

Microsoft is still investigating this issue. Thus, until a security patch or a directive from the vendor is available you should follow the below workarounds:

Prohibit the installation of new ActiveX controls by adding a few keys to the system registry: (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444).

Disabling the installation of all ActiveX controls in Internet Explorer mitigates this attack. This can be accomplished for all sites by configuring the Group Policy using your Local Group Policy Editor or by updating the registry. Previously-installed ActiveX controls will continue to run, but do not expose this vulnerability.

To disable ActiveX controls via Group Policy

In Group Policy settings, navigate to Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page

For each zone:

• Select the zone (Internet Zone, Intranet Zone, Local Machine Zone, or Trusted Sites Zone).

• Double-click Download signed ActiveX controls and Enable the policy. Then set the option in the policy to Disable.

• Double-click Download unsigned ActiveX controls and Enable the policy. Then set the option in the policy to Disable.

We recommend applying this setting to all zones to fully protect your system.

You should understand the importance of security updates, and the urgency with which they should be applied, no matter how large or small your organization is. It is very important to apply an efficient patch management solution and always have enabled an active event security logging and practice event monitoring. To protect the valuable assets of your business and be compliant with the relevant industry regulations requires a comprehensive approach to the management of risk, including Penetration Testing at least annually and upon significant changes.

References:

- https://thehackernews.com/2021/09/new-0-day-attack-targeting-windows.html?&web_view=true
- https://www.techworm.net/2021/09/zero-day-windows-microsoft-office-document.html
- https://www.odysseycs.com/threat-alert/new-0-day-attack-targeting-windows-users-with-microsoft-office-documents