

Forum: [Hack Forums](#)

Thread: [Office CVE-2021-40444 remote code execution native builder](#)

mimikatz - September 10, 2021, 2:59 pm

as there is no any available builder for this

CVE-2021-40444 remote code execution vulnerability in MSHTML

Office 2019 / Office 365 on Windows 10 (typical user environment)

The exploit uses logical flaws so the exploitation is perfectly reliable

the rendering engine used by IE and succeeded by EdgeHTML in the newer Edge browser

there is no patch there is only Defender Antivirus detection and i managed to bypass it.

the only way to stop the attack is disabling installation of all ActiveX controls in IE.

the vulnerability in RTF files, which do not benefit from Office's Protected View security feature.

DEMO : <https://streamable.com/pt7rwp>

mail : darkc0d3s@protonmail.com

[contract=tid]Start Contract[/contract]

mimikatz - September 13, 2021, 6:10 am

i do not know why people giving you flame -rep without any reason when you try to sell something here !

account_ - September 13, 2021, 6:13 am

(Sep 13, 2021 06:10 AM)mimikatz Wrote: [CITE](#) i do not know why people giving you flame -rep without any reason when you try to sell something here !

Pop does not matter, its more about the B ratings.

ziriolo2020 - September 13, 2021, 9:48 pm

Really cool!! What is the price of this script?

mimikatz - September 14, 2021, 6:15 am

its 1100usd and updating from detections for 3 months

bat777 - September 27, 2021, 12:42 am

this man don't want to escrow. mb ripper