

Forum:[Hack Forums](#)

Thread: [Looking for Silent .doc exploit.](#)

KKM112244 - July 3, 2024, 5:41 am

Can someone refer me to a reliable silent .doc exploit ..

DramaKing - July 3, 2024, 5:42 am

I suppose you want something newer than 2010?

KKM112244 - July 3, 2024, 5:45 am

(Jul 3, 2024 05:42 AM)DramaKing Wrote: [\[CITE\]](#) I suppose you want something newer than 2010?

Yeah do you know any ?

DramaKing - July 3, 2024, 5:56 am

(Jul 3, 2024 05:45 AM)KKM112244 Wrote: [\[CITE\]](#) Yeah do you know any ?

Since you didn't take the hint, here's an exploit that you can use if your footprinting shows this specific version of the MS 365 Outlook app in use: [Microsoft Office 365 Version 18.2305.1222.0 - Elevation of Privilege + RCE](#). You sound very inexperienced, so let me warn you that playing with exploits like these is not script kiddie-level hacking.

Oh, one more thing: MS 365 / Office 365 is automatically updated. You know about patches, right?

bujumurderer - July 10, 2024, 4:32 pm

(Jul 3, 2024 05:41 AM)KKM112244 Wrote: [\[CITE\]](#) Can someone refer me to a reliable silent .doc exploit ..
i have it

Binance - July 10, 2024, 4:40 pm

(Jul 3, 2024 05:41 AM)KKM112244 Wrote: [\[CITE\]](#) Can someone refer me to a reliable silent .doc exploit ..

There are none working in modern day
please do not trust the guy above. this is most common scam in cybercrime.

do not trust any youtube video or even "live demo" of builder.

Since 2018 these have taper off.
since 2020 these became myths. now they are sold for 500k +. 1m+ for RCE/HTA.
this is a 0day

use logic bro
.doc exploits have had there day and gone.

Bastille - July 10, 2024, 10:57 pm

The last one I've heard about was Follina in 2022 :

<https://gauthamprasath.medium.com/follina-msdt-vulnerability-cve-2022-30190-analysis-and-poc-29f61cd2c07f>

Binance - July 11, 2024, 6:47 am

(Jul 10, 2024 10:57 PM) Bastille Wrote: [\[CITE\]](#) The last one I've heard about was Follina in 2022 :

<https://gauthamprasath.medium.com/follina-msdt-vulnerability-cve-2022-30190-analysis-and-poc-29f61cd2c07f>

Follina was never for sale as bypassing any AV. And did not allow drop of execution of .exe or .ps1 script.

It needed to be staged and bundled with a suite of other malwares to become dangerous.

FreakCanReallyDolt - July 21, 2024, 3:00 pm

I know a simple trick you can use smbrelay.py with a \\ to your server ip and use smbrelay to hijack machine. works with latest pdfs.