

Forum:[Hack Forums](#)

Thread: [USG CRYPTER CVE 2017 8759 Exploit Full TUT](#)

YAK_CODER - September 28, 2017, 5:05 am

USG CRYPTER CVE 2017 8759 Exploit TUT

<https://www.youtube.com/watch?v=LFleBQuqWGc&feature=youtu.be>

download files

<http://www83.zippyshare.com/v/ND1y8UDQ/file.html>

pass on file name

<http://the-nightmare.com>

add me

icq:716557549

skype:kareem.alex1

skype group: <https://join.skype.com/pr98CGrcUfbu>

Zens - September 28, 2017, 7:49 am

Quote:Purple Kief (134) Neutral (0): Infecting HF members is a no-no. 01-09-2017,07:11

Linux™ (214) Negative (-3): Stop trying to infect people 01-09-2017, 05:14

Oh, nice try nice try

DO NOT DOWNLOAD THIS SKETCHY THING

ken0man - September 28, 2017, 8:13 am

what is the file password? the pass you gave is not working

MaDTiA - September 28, 2017, 8:22 am

(Sep 28, 2017 08:13 AM)ken0man Wrote: [\[CITE\]](#) what is the file password? the pass you gave is not working

don't download it man seriously

YAK_CODER - September 28, 2017, 9:46 am

(Sep 28, 2017 08:22 AM)Wr_Retail Wrote: [\[CITE\]](#) don't download it man seriouslyReally?

who is this Purple Kief ?

stop bieng asshole

and watch the fuckin video to learn somthing

(Sep 28, 2017 08:13 AM)ken0man Wrote: [\[CITE\]](#) what is the file password? the pass you gave is not workingon zippyshare look into file name its on it

Baud - September 28, 2017, 11:11 am

I don't see anything shady in this, the file looks clean from nodistribute, I'm not going to open it until I move it to my VPS but it looks like a legit exploit. Although the AutoOpen() function can trigger a few anti virus when your target opens the .doc.

YAK_CODER - October 2, 2017, 2:28 am

(Sep 28, 2017 11:11 AM)Baud Wrote: [\[CITE\]](#) I don't see anything shady in this, the file looks clean from nodistribute, I'm not going to open it until I move it to my VPS but it looks like a legit exploit. Although the AutoOpen() function can trigger a few anti virus when your target opens the .doc. Thas how real hacker Review something

john_theDarkLord - October 2, 2017, 3:31 am

what is that?? Macro? Really? its just a simple Poc,its not cve.do not full the members please.If you want call objects in macro there are a lot of easy ways to do that.

Tsukiri - October 2, 2017, 3:34 am

CVE 2017 8579 is an exploit which allows you to create a silent .doc, it has been released on github by bhdresh. If the thing OP posted contains an exe or anything other than a .txt or .py, then do not open it. The builder is coded in .py (heavily detected though).

Alright I checked it out, and indeed, this is not backdoored as far as I can see. (wouldn't run it on my own PC though).

However, I think this guy made a silent exploit into a macro. Normally, the file output from CVE 2017 8579 has a .RTF structure.

This file however has a .doc file structure (which isn't possible to exploit using this particular exploit).

He is calling the download & execution using a macro, meaning that the whole idea of a silent exploit has been defeated.

I'm sorry OP but this is useless, unless I am wrong.

For those wondering, this is the AV scan: <http://viruscheckmate.com/id/jA3YXQvGtZtt>

The macro is the thing raising the detection though. The version OP shared is a silent exploit technique to link the payload

combined with a macro to actually run the exploit, making it useless, since using a normal macro would be much easier, would always work if they enable macro's, and is FUD (atleast, mine is).

Also, since this "macro" thing or however you want to call it is based on a silent exploit, it won't execute on systems that have the latest patch installed.

AKA, just use a macro. Even though this is not a bad thing to learn from and 2/40 scantime for free isn't that bad either (however I think it won't bypass at runtime since it's using a simple VBS downloading script).

YAK_CODER - October 2, 2017, 6:33 am

(Oct 2, 2017 03:34 AM)Tsukiri Wrote: [\[CITE\]](#) CVE 2017 8579 is an exploit which allows you to create a silent .doc, it has been released on github by bhdresh. If the thing OP posted contains an exe or anything other than a .txt or .py, then do not open it. The builder is coded in .py (heavily detected though).

Alright I checked it out, and indeed, this is not backdoored as far as I can see. (wouldn't run it on my own PC though).

However, I think this guy made a silent exploit into a macro. Normally, the file output from CVE 2017 8579 has a .RTF structure.

This file however has a .doc file structure (which isn't possible to exploit using this particular exploit).

He is calling the download & execution using a macro, meaning that the whole idea of a silent

exploit has been defeated.

I'm sorry OP but this is useless, unless I am wrong.

For those wondering, this is the AV scan: <http://viruscheckmate.com/id/jA3YXQvGtZtt>

The macro is the thing raising the detection though. The version OP shared is a silent exploit technique to link the payload

combined with a macro to actually run the exploit, making it useless, since using a normal macro would be much easier, would always work if they enable macro's, and is FUD (atleast, mine is).

Also, since this "macro" thing or however you want to call it is based on a silent exploit, it won't execute on systems that have the latest patch installed.

AKA, just use a macro. Even though this is not a bad thing to learn from and 2/40 scantime for free isn't that bad either (however I think it won't bypass at runtime since it's using a simple VBS downloading

script). Good review

but i dont share all my idia yet

look for those guys they plam me to spread virus?

how the fuck i can give them moor

Tsukiri - October 2, 2017, 8:13 am

(Oct 2, 2017 06:33 AM)crypt4u Wrote: [\[CITE\]](#) Good review

but i dont share all my idia yet

look for those guys they plam me to spread virus?

how the fuck i can give them moor

It's not really about an "idea". This file isn't an obfuscated exploit, either.

The exploit only works in .RTF file structures and this is a .doc file (structure).

Meaning that you aren't using an exploit at all.

I don't really think you have a clue what you're talking about to be honest. Your English is completely broken and even the topic title is ridiculous. "USG CRYPTER"? What does that have to do with anything you've shown us? You don't "crypt" an exploit, you change the code so that it doesn't get recognized by the AV vendor.

It's not like you can just encrypt the exploit source using RC4 and make it FUD like that, lol.

avalanche - August 27, 2018, 2:27 pm

nice one... hope this product is till on sell?