

## Forum:[Hack Forums](#)

Thread: [CVE EXPLOIT KIT \(MICROSOFT OFFICE, ADOBE FLASH & WINDOWS RDP\)! \[LIMITED QUANTITY\]](#)

**Nyugen3** - October 23, 2019, 4:18 pm

Howdy ya""lllll!

I am selling an exploit kit containing the following CVEs:

CVE-2012-0158

CVE-2017-0199

CVE-2017-0213

CVE-2017-0262

CVE-2017-8570

CVE-2017-11882

CVE-2018-4878

CVE-2018-15982

CVE-2019-0708

CVE-2012-0158 is being sold for use with Microsoft Office 2003 (SP3) and Microsoft Office 2007 (SP2/SP3). When exploited, arbitrary code execution is gained for the compromised process.

CVE-2017-0199 is being sold for use with Microsoft Office 2007 (SP3), Microsoft Office 2010 (SP2), Microsoft Office 2013 (SP1) and Microsoft Office 2016. When exploited, arbitrary code execution is gained for the compromised process.

CVE-2017-0213 is being sold for use with Windows 7 (SP1), Windows 8.1 and Windows 10 (Builds 1511, 1607 and 1703). When exploited, escalation of privilege occurs (abusing COM for this).

CVE-2017-0262 is being sold for use with Microsoft Office 2010 (SP2), Microsoft Office 2013 (SP1) and Microsoft Office 2016. When exploited, arbitrary code execution is gained for the compromised process.

CVE-2017-8570 is being sold for use with Microsoft Office 2007 (SP3), Microsoft Office 2010 (SP2), Microsoft Office 2013 (SP1) and Microsoft Office 2016. When exploited, arbitrary code execution is gained for the compromised process.

CVE-2017-11882 is being sold for use with Microsoft Office 2016 only, but Microsoft Office 2007 (SP3), Microsoft Office 2010 (SP2) and Microsoft Office 2013 (SP1) are also affected by this vulnerability.

CVE-2018-4878 is being sold for use with Adobe Flash Player (any version prior build 28.0.0.161). When exploited, arbitrary code execution is gained for the compromised process.

CVE-2018-15982 is being sold for use with Adobe Flash Player (any version prior build version 31.0.0.153). When exploited, arbitrary code execution is gained for the compromised process.

CVE-2019-0708 is being sold for use with Windows XP, Windows Server 2003, Windows Vista, Windows 7 and Windows Server 2008. When exploited, arbitrary code execution is gained for the compromised target. This vulnerability requires Remote Desktop Services to be enabled on the machine and is exploited by sending certain network packets to the target via Remote Desktop Services support.

I have uploaded some samples which I have modified to exploit some of these vulnerabilities to VirusTotal because the CVEs are known and Anti-Virus vendors already have generic signatures for them. This does not mean you cannot FUD the exploitation of these vulnerabilities - I can help you do this if you are a client of mine for no additional cost.

[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)  
[VirusTotal](#)

I am not selling individual CVEs, I am selling the whole lot as a kit, so please do not waste my time asking to purchase only one or a few of them.

The purchase is for full access to any demonstration samples, source-code access to a utility which will take a file input and spit back out a new copy which has been modified to exploit the appropriate vulnerability and source-code access to any payloads (most are native). Payloads for use with any arbitrary code execution are automatically included (e.g. downloader).

There is a limited quantity of sales available.

Exclusive sale: \$800.

Standard sale: \$250.

The exclusive sale is only available until someone has purchased a standard sale and is for being the only client of mine for this kit. Once someone has purchased a standard sale, the exclusive sale cannot be offered anymore because then it wouldn't be exclusive.

Thank you.

[contract=tid]Start Contract[/contract]

Exe - October 23, 2019, 4:49 pm

Oof oof lets see how this sale thread goes

**FourierFive** - October 24, 2019, 4:03 am

Send me over a PM, don't have 25 post yet.

**Nyugen3** - October 24, 2019, 9:47 am

(Oct 24, 2019 04:03 AM)FourierFive Wrote: [\[CITE\]](#) Send me over a PM, don't have 25 post yet.I've sent you a PM. Hopefully you will be able to reply to them. If you cannot then notify me again here.

**k1ng0fn0th1ng** - October 24, 2019, 10:04 am

Is that a bunch of public stuffs collected by you in one folder?

How is that look like? Some kind of builder?

Can you provide some video proofs of exploiting some of these CVEs?

**Nyugen3** - October 24, 2019, 12:21 pm

(Oct 24, 2019 10:04 AM)k1ng0fn0th1ng Wrote: [\[CITE\]](#) Is that a bunch of public stuffs collected by you in one folder?

How is that look like? Some kind of builder?

Can you provide some video proofs of exploiting some of these CVEs?1. It's not a "bunch of public stuffs collected ... in one folder". There might already be information or PoCs for countless CVEs but there's a difference between PoC and real-world exploitation. There's a lot of things that need to be handled for compatibility and reliability that isn't of concern for most PoCs in general.

2. If you're referring to the utility I mentioned, it's a simple GUI application that allows you to select the CVE, select an input file and select an output file, along with options on the payload (e.g. you can specify shellcode manually for the arbitrary code execution CVEs or use pre-ready payloads). File format checks are performed to help prevent user error.

3. No, there aren't any videos at this moment in time.

**FourierFive** - October 24, 2019, 5:10 pm

I will buy the standard package, this is some high quality stuff.

**Nyugen3** - October 24, 2019, 5:12 pm

A standard sale has already been sold now so there is no exclusive package available anymore.

The price of the standard sale is being moved from \$250 to \$150 and there is a quantity of five sales available.

(Oct 24, 2019 05:10 PM)FourierFive Wrote: [\[CITE\]](#) I will buy the standard package, this is some high quality stuff.Initiate the contract with the button on the original post. The price is lower as you can see from my note above. I will send you a PM also.

Edit: There will be a quantity of four now.

**knockingonheavensdoor** - October 25, 2019, 12:32 am

These exploits are already freely available on Github.

<https://github.com/houjingyi233/office-exploit-case-study/tree/master/CVE-2012-0158%26CVE-2012-1856/CVE-2012-0158>

[GitHub - bhdresh/CVE-2017-0199: Exploit toolkit CVE-2017-0199 - v4.0 is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft Office RCE. It could generate a malicious RTF/PPSX file and deliver metasploit / meterpreter / other](#)

[payload to victim without any complex configuration.](#)

[Exploits/CVE-2017-0213 at master · WindowsExploits/Exploits · GitHub](#)

<https://github.com/houjingyi233/office-exploit-case-study/tree/master/CVE-2017-0261%26CVE-2017-0262>

[GitHub - rxwx/CVE-2017-8570: Proof of Concept exploit for CVE-2017-8570](#)

<https://github.com/houjingyi233/office-exploit-case-study/tree/master/CVE-2017-11882%26CVE-2018-0802%26CVE-2018-0798>

[GitHub - anbai-inc/CVE-2018-4878: CVE-2018-4878](#)

[Exploit/CVE-2018-15982 at master · 0xR0/Exploit · GitHub](#)

[GitHub - Ekultek/BlueKeep: Proof of concept for CVE-2019-0708](#)

**Nyugen3** - October 25, 2019, 5:25 am

(Oct 25, 2019 12:32 AM)knockingonheavensdoor Wrote: [\[CITE\]](#) These exploits are already freely available on Github.

<https://github.com/houjingyi233/office-exploit-case-study/tree/master/CVE-2012-0158%26CVE-2012-1856/CVE-2012-0158>

[GitHub - bhdresh/CVE-2017-0199: Exploit toolkit CVE-2017-0199 - v4.0 is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft Office RCE. It could generate a malicious RTF/PPSX file and deliver metasploit / meterpreter / other payload to victim without any complex configuration.](#)

[Exploits/CVE-2017-0213 at master · WindowsExploits/Exploits · GitHub](#)

<https://github.com/houjingyi233/office-exploit-case-study/tree/master/CVE-2017-0261%26CVE-2017-0262>

[GitHub - rxwx/CVE-2017-8570: Proof of Concept exploit for CVE-2017-8570](#)

<https://github.com/houjingyi233/office-exploit-case-study/tree/master/CVE-2017-11882%26CVE-2018-0802%26CVE-2018-0798>

[GitHub - anbai-inc/CVE-2018-4878: CVE-2018-4878](#)

[Exploit/CVE-2018-15982 at master · 0xR0/Exploit · GitHub](#)

[GitHub - Ekultek/BlueKeep: Proof of concept for CVE-2019-0708](#) This has already been addressed in the thread, you're not telling us anything new.

Quote: There might already be information or PoCs for countless CVEs but there's a difference between PoC and real-world exploitation. There's a lot of things that need to be handled for

compatibility and reliability that isn't of concern for most PoCs in general.

I can say it again in different words if it helps other people understand, but my advice would be to touch up on your English skills and read the thread prior to replying to it in the future:

There is a big difference between Proof-of-Concept exploitation. More often than not, they are not going to be very reliable.

Proof-of-Concept exploits are almost always going to be flagged by Anti-Virus vendors (who will be using generic signatures for static and dynamic memory scanning) and the solution to this is not always as simple as others on this forum usually like to believe is the solution to everything: "just run it through an FUD crypter!". In the real-world, you do not want to have high entropy when exploiting a vulnerability, which means avoiding obfuscation/packing/any alternate "crypter" technique, because this stands out more than a brand new Ferrari does. There are better ways to make something remain "FUD" (to a reasonable extent, because you will never truly know if something is "FUD" to everything in the world, and detection algorithms change on a regular basis), like keeping it unique without applying the same old tricks that everyone has known for decades, that will raise the scoring of things like entropy.

Furthermore, reliability is not just about surpassing Anti-Virus detection. It is also about environment compatibility. Preferably, you will want support on ARM, Intel and AMD systems as well as numerous versions of Windows and the targeted software (e.g. if it isn't an OS vulnerability). This requires additional use-case handling which often has to be done manually.

Last but not least, moving away from the point of reliability, essentially all of the work is already being done for you. You would be getting the payloads to use with the CVEs, preventing you from having to develop your own payload which will be compatible with the chosen CVE and will be reliable on the supported targets (the payload may also have to be different for compatibility across multiple targets of the same software in terms of build depending on the circumstances), and this also brings less hassle regarding detection of those payloads.

No one on the forum is being forced to purchase the CVE exploit kit but a few have and appear to be happy with what they have received. It is normal for there to be public documentation and proof-of-concepts of CVEs online (and once a CVE has been used in a malware campaign, more details are often provided on research blogs which help other security researchers create public proof-of-concepts for them). I do not understand why it comes as a shock to people on this forum that the CVEs I am selling are already known and most or all of them already have public proof-of-concepts for them, after all, the CVE is public for me to know the CVE and I had to find research on them to exploit them unless I magically were to figure out what was being exploited for that CVE (which usually is going to be unlikely for anyone unless the CVE documentation provides a lot of details, which isn't common).

Everyone has a right to continue re-iterating what has been said, but I'd appreciate it if people stopped wasting my time with it or trying to make out like I am being unorthodox for selling CVEs which already have public proof-of-concepts, because I am not selling public proof-of-concepts. It is irrelevant as to whether there is already a public proof-of-concept for a CVE that I am selling, because it isn't going to be the same thing that I am selling. Be my guest to use the public proof-of-concepts yourself if that is what you deem sufficient, but in the real-world, it's going to be a lot more complicated than using some open-source proof-of-concepts if you want compatibility/reliability and want to clean up the tracks you'll be leaving behind.

I have even taken the time to address dynamic exploit mitigation software like HitmanPro.Alert, etc. This is also another example of something that is not addressed in any of these public CVE

proof-of-concepts, other than generic mitigation's like getting around ASLR or DEP (which is usually not going to be addressed when the targeted software is not actively using those mitigation's of it's own choice, which would cause an issue if exploit protection software was enforcing it automatically and the targeted software was still able to function with these forced mitigation's). Like I have said, there are a lot of use-cases to handle for reliability.

Thank you.

**Nyugen3** - *October 26, 2019, 7:13 am*

Bump

Selling only two more copies of the CVE Exploit Kit for \$150 \$100 in BTC!

**Nyugen3** - *October 27, 2019, 8:37 am*

(Oct 27, 2019 07:42 AM)omar18881 Wrote: [\[CITE\]](#)

So you basically selling CVE's that are shared freely on Github , Just Wow ? , didn't know your Mighty CVE exploit kit are all from Github ? ? You're emotional because I called you out on another thread. Stop flaming and read the thread. I'm not using anything from GitHub and it isn't just the CVEs you're getting.