

Rule of Zer0Fest2018 Spring

(Last updated: January 1, 2018)

Zer0Fest("Contest", <http://www.zer0fest.org>) is organized by POC Security("Organizer"). The Contest will be held in Zer0Con(<http://www.zer0con.org>) and POC(<http://www.powerofcommunity.net>) every year. **Zer0Fest2018 Spring will be held at the K-Hotel on March 29th ~ 30th, 2018 during Zer0Con2018 in Seoul, Korea.**

The purpose of Zer0Fest is to make vendors more responsible, to make bug hunters more respected, and to make the world much safer.

Eligibility

- There is no limitation on the participants' registration except for employees of Organizer.
- A participant is not eligible for the products of his own company.
- A participant must provide valid and accurate information which will be included in the registration form provided by Organizer. If the information provided by the participant is not true, the participant may be disqualified. Organizer has a right to decide the disqualification of any participant.
- Employees of target vendors and their respective affiliates, subsidiaries, related companies are also eligible to participate in Contest except their own products. And a judge are also eligible to participate in Contest except the target that he is appointed as a judge.
- If a vulnerability has been reported to a vendor or sold to 3rd parties, any participant with the vulnerability is not eligible.

Registration

- A participant can register on the Contest website(<https://goo.gl/QgVXjZ>).
- In case of some problems occurred in the website, a participant can contact through Organizer (pocadm@gmail.com) directly with the following information: name, email address, his target(s). And then, Organizer will get in contact with the participant directly.
- **The deadline of registration is 24:00(UTC+09), March 23, 2018.**

Online Participation

A participant can participate online. If a participant does not present at the venue but willing to participate online, he or she must send Organizer all information including detailed technical paper and exploit code by March 26, 2018.

The technical paper must include step-by-step exploitation process. Judges will check if the vulnerability is exploitable with the exploit code of the participant during Contest. Organizer will keep all information closed that online participants submit.

The order of exploitation of online participants is also decided by the same rule as the order of offline participants when they have a same target.

A free ticket for POC and an invitation to Zer0Con registration will be given to all online participants who submit detailed information and exploit code.

Targets and Prize

All targets and related operation systems will be updated to the latest and fully patched version available no later than 24:00(UTC+09), March 28, 2018. All target software will be installed and configured as the default configuration.

The targets are divided into two categories:

Target Category-1 is basically rewarded by Organizer, sponsors, and vendors.

Target Category-2 is rewarded only by vendors.

If any participant who has 0-days wants to add new target(s), he can contact and ask [Organizer by March 20, 2018](#). If new targets are added, the target list will be updated.

If a participant is not satisfied with the reward that vendors suggest or vendors don't pay, the participant does not need to submit his research to Organizer. Judges only will decide the existence of any bugs and notice the existence of the bugs and name of participants in the internet for credit and profit of the participants. The participant can do at his own disposal. This is for the sake of bug hunters' profit and fame.

The blanks of two reward parts will be updated by **March 20, 2018**. And the reward may be increased if any sponsors will join to support the reward. The more sponsors, the more reward. The reward starts with Basic Reward on January 1, 2018 and Organizer will keep updating it. The final reward will be decided on March 20, 2018.

[Target Category - 1]

Last updated: January 5, 2018

Vendor	Target	Basic Reward	Vendor Reward
Microsoft	Windows 8.1 / 10	RCE to system	
		LPE to System	
	Edge	RCE, Sandbox bypass / escape	
	IIS 7, 8	RCE	
	Office	RCE, Sandbox bypass / escape	
Apple	macOS	RCE	
		LPE	
	Safari(macOS)	RCE, Sandbox bypass / escape	
	Safari(iOS)	RCE, Sandbox bypass / escape	
	iOS(latest)	RCE, Privilege escalation	
Google	Chrome(Win)	RCE, Sandbox bypass / escape	
	Chrome(other OS)	RCE, Sandbox bypass / escape	
	Android 7.x, 6.x	RCE, Privilege escalation	
Mozilla	Firefox with TOR	RCE, Sandbox bypass / escape	
Samsung	Galaxy S8, Note8	RCE, Privilege escalation	
LG	V30	RCE, Privilege escalation	
VMWare	Workstation, Fusion	Guest-to-Host escape	
Adobe	Flash Player	RCE, Sandbox bypass / escape	
	PDF Reader	RCE, Sandbox bypass / escape	
	CentOS(latest)	RCE to root	
		LPE to root	
	Ubuntu(latest)	RCE to root	
		LPE to root	

ETC	Apache Web Server	RCE		
	PHP	RCE, Information Disclosure		
	Dovecot	RCE, Information Disclosure		
	Postfix	RCE, Information Disclosure		
	Sendmail	RCE, Information Disclosure		

[Target Category - 2]

Vendor	Target	Basic Reward	Vendor Reward
SNS	Facebook	Any	
	Twitter	Any	
Messenger	Kakaotalk	RCE / LPE	
	Signal	RCE / LPE	
	Telegram	RCE / LPE	
	Threema	RCE / LPE	
	Wechat	RCE / LPE	
Network Device	WhatsApp	RCE / LPE	
	Cisco	RCE	
	D-Link	RCE	
	Huawei	RCE	
	IBM	RCE	
	Juniper	RCE	
	Linksys	RCE	
Antivirus	TP-Link	RCE	
	AhnLab	RCE	
	Bitdefender	RCE	
	Kaspersky	RCE	
	McAfee	RCE	
	Symantec	RCE	
	TrendMicro	RCE	

	WinDefender	RCE		
	Qihoo360	RCE		
ETC	Apple Pay	Any		
	AliPay	Any		
	Hancom Office	Any		
	SamSung Pay	Any		

In the case of network devices, judges will check the technical papers submitted by participants. If he wants to bring the target devices, he must inform Organizer to bring them before two weeks before Contest. Judges can check the devices for the sake of fair contest management.

A Best Hacker, the contestant who succeeds in pwning his target(s) with best techniques will be awarded with a chance to attend POC2018 and Zer0Con2019 for free. Organizer and judges will decide who gets the reward based on their technical performance and announce at the closing ceremony of Zer0Con2018.

Sponsor(s)

For more information about Zer0Fest Sponsorship, contact Organizer to "pocadm@gmail.com" with PGP key(<http://zer0fest.org/poc.asc>).

Determination of the Successful Demonstration

To win the reward, firstly, a participant must exploit initial vulnerability within the target software, and use it to modify the normal execution path of the software in order to get the remote arbitrary code execution allowed in this software. Secondly, the demonstration must be finished during the process of viewing the contestant controlled website by using a browser (the default one, if it's not specified); besides this, any other user interaction is not allowed. The only thing allowed is to enter the URL on browser interface and navigate to it.

After a successful remote code execution, the demonstration must contain a payload which can bypass the application sandbox to execute in the elevated security context that allows the payload to have rights to read, write, and delete data which is inaccessible inside the sandbox. The demonstration must prove that the payload can

successfully get such kind of rights. For example, on Windows targets, the contestant may choose to run a command line tool with Medium integrity level, and for iOS target, the contestant may present the sensitive information of other application. The contestant can choose any methods they like but the methods must meet the above requirements clearly.

To be a Best Hacker, the payload should bypass the application sandbox to get system/root/kernel level rights that can access the system resources or functionalities which only can be accessible under the system/root/kernel level permission. The demonstration must prove that the payload can successfully get such kind of rights. For example, on Windows targets, the contestant may choose to run a command line tool with System integrity level, and for iOS target , the contestant may install a system application. he contestant can choose any methods they like but the methods must meet the above requirements clearly.

To win the reward in the virtual machine targets, the demonstration must use the vulnerabilities within the virtual machine software and use it to modify the normal execution path of the host process of virtual machine software in order to get the arbitrary code execution allowed in this process. The demonstration must be finished by running an exploit program inside the guest operation system.

The demonstration must prove that the exploit program can successfully run an arbitrary code in the context of virtual machine host process. For example, the contestant may choose to run a command line tool in host operation system. The contestant can choose any methods they like, but the methods must meet the above requirements clearly.

Restriction of Vulnerability Reuse

Regardless of how many targets one contestant participates in, a vulnerability can be used only once for all categories.

Multiple Contestants in One Target

If two or more contestants registered for the same target, we will draw a random order for them. Dice will be rolled by Organizer to decide the contest order. The one who get the most dots will be the first and the rest will be done in the same manner.

Only the first team that succeeds will get full reward money. For the second and the rest teams, if vendors are willing to offer reward money, the contestant will be noticed before starting the demonstration, otherwise, there will be no reward money.

Time Limitation

A contestant will have 3 exploit attempts during his demonstration; each attempt must be finished within 4 minutes. The time used for network and device configuration will not be counted.

Vulnerability and Exploit Review

After successful demonstration of the exploit, the contestant must provide Organizer with a detailed document that describes all the vulnerability, technical information, and step-by-step exploit technique and process used in the exploit as well as the complete exploit source code which is used in the demonstration.

A target vendor can join the exploit review and get all information if the vendor will pay reward money for a participant. If the vendor will not pay, the vendor can't get any chance to join the exploit review and get information about the vulnerability.

As previously mentioned, if a participant is not satisfied with the reward that vendors suggest or vendors don't pay, the participant does not need to submit his research to Organizer. Judges only will decide the existence of any bugs and notice the existence of the bugs and name of participants in the internet for credit and profit of the participants. The participant can do at his own disposal.

The vulnerability and exploit information will be disclosed to the judges who come from both target vendors and Organizer. They keep the right to decide whether the contestant successfully compromised the target or not, by checking the whole process of the demonstration and reviewing information provided by the contestant.

The vulnerability used in the exploit must not be known to any other 3rd parties including target software vendors before the reviewing; otherwise, there will be no reward for the contestant.

A winner must keep all information about his vulnerability, exploit technique, and exploit

code in strict confidence before vendors patch them. If he discloses any information about the vulnerability, Organizer will not pay reward money.

Prize Remittance

Organizer will remit all reward within two months. And If vendors decide to pay vendors' reward, vendors and participants can agree the payment term but the term must be within 2 months. The way to pay will be decided by mutual agreement of vendors and participants.

If Organizer pays participants reward, the ownership of the vulnerabilities is at Organizer's. Participants must not open his bug information for 6 months for the sake of security. After 6 months, participants can use his bug at his own purpose.

Miscellaneous

- By participating in Contest, a participant must warrant that he is a sole owner of all the rights related to his vulnerability and exploit.
- A participant must warrant that his vulnerability has not been reported to vendors or third parties.
- The contestant is responsible for any kind of legal problems which may occur from his trials to compromise targets.
- All participants agree to fully indemnify Organizer from any and all claims by third parties in relation to Contest.
- Organizer may cancel Contest without prior notice in the case of force majeure causes that are beyond the reasonable control of Organizer, including but not limited to fire, storm, earthquake, wars, revolutions, riots, civil commotion, national emergency, and act or order of any court, government or government agency.
- Organizer can use contestant's information including but not limited to name, email, phone number only for the sake of running Contest properly.

- Organizer reserves the right to change the rules of Contest for more reasonable Contest administration and participants' profit without notice.
- Organizer will contact participants and notice on the website if any changes happen.
- These Terms shall be governed by and construed in accordance with the laws of Republic of Korea. If any disputes arise out of or in connection with these Terms, participants agree to submit to the exclusive jurisdiction of the Korea courts