Rule of PwnFest2016

PwnFest 2016("Contest") is organized by POC("Organizer") and Sponsors("Sponsor"). It will be held at the K-Hotel during POC2016 conference(Nov. 10th ~ 11th, 2016) in Seoul, Korea.

Eligibility

- Contest doesn't put any 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 rights to decide the disqualification of any participants.
- Employees of sponsors and their respective affiliates, subsidiaries, related companies, and judges are also eligible to participate in Contest. However, a judge is not eligible to participate as a contestant in the target that he is appointed as a judge.

Registration

- A participant can register on the Contest website.
- 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), November 5th, 2016.

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), Wednesday, November 9th, 2016. All target software will be installed and configured as the default configuration.

Targets	Basic Reward	Extra Reward
Microsoft Edge + Windows 10 x64 RS1	USD $120,000	USD $20,000
Microsoft Hyper-V + Windows Server 2016	USD $150,000	N/A
Google Chrome + Windows 10 x64 RS1	USD $120,000	USD $20,000
Android 7.0 + Google Pixel	USD $120,000	USD $20,000
Adobe Flash + Microsoft Edge + Windows 10 x64 RS1	USD $100,000	USD $20,000
Apple Safari + macOS Sierra	USD $80,000	USD $20,000
Apple iOS 10 + iPhone 7 Plus	USD $120,000	USD $60,000
VMWare Workstation Pro 12 + Windows 10 x64 RS1	USD $150,000	N/A

The total reward pool offered by the Sponsor is 1.7 million USD.

Targets	Basic Medal	Extra Medal
Microsoft Edge + Windows 10 x64 RS1	3	1
Microsoft Hyper-V + Windows Server 2016	7	N/A
Google Chrome + Windows 10 x64 RS1	3	1
Android 7.0 + Google Pixel	3	1
Adobe Flash + Microsoft Edge + Windows 10 x64 RS1	3	1
Apple Safari + macOS Sierra	2	1
Apple iOS 10 + iPhone 7 Plus	3	2
VMWare Workstation Pro 12 + Windows 10 x64 RS1	6	N/A

A ***Lord of Pwn***, the contestant who owns the most medals will be awarded with a gold trophy. If two or more teams get the same number of medals, Organizer and Sponsor will decide who gets the trophy based on their technical performance.

Determination of the Successful Demonstration

For Windows, macOS, iOS, and Android Targets:

To win the basic reward and medals, firstly, the demonstration must exploit an initial vulnerability within the target software, and use it to modify the normal execution path of the software in order to get the remotely 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 win the extra reward and medals of the targets, 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.

For Virtual Machine Targets:

To win the reward and medals, 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 a Windows 10 x 64 guest operation system. The operation system running in the host will be Windows 10 x64 or Windows Server 2016.

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.

For the first succeed team, Sponsor will offer the full value of reward money and medals. For the second and the rest teams, if Sponsor or vendors are willing to offer reward money, the contestant will be noticed before starting the demonstration, otherwise, there will be no reward money but medals only.

 # 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 the Organizer and the Sponsor with a detailed document that describes all the vulnerability, technical information, and step-by-step exploit technique used in the exploit as well as the complete exploit source code which were used in the demonstration.

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.

To avoid any dissent between contestants and judges, there will be a technical committee consisted of 5 consultants who enjoy great reputation in this community. These experts will be selected and announced by Organizer. And there will be a principle consultant appointed by Organizer before Contest. If there are any dissents, this technical committee will vote anonymously for an amicable settlement.

The vulnerability used in the exploit must not be known to any other 3rd parties including target software vendors and the Sponsor before the reviewing; otherwise, there will be no reward for the contestant. If the vulnerability is previously disclosed only to vendors, the contestant still has a chance to get medals.

Security experts from Sponsor will also join the reviewing process; however, they have no right to interfere the judgment. Sponsor keeps the right to offer extra reward even if the exploit provided by contestants doesn't meet the above requirements.

A winner must keep all information about his vulnerability, exploit technique, and exploit code in strict confidence before vendors patch them.

Vendors reserve the right to offer extra reward to contestants for special targets added for the sake of testing beta version of their products.

Prize Remittance

Prize will be remitted after 8 weeks of Contest. The Sponsor and the contestants are responsible for respective taxes

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.

- 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 and Sponsor from any and all claims by third parties in relation to Contest.
- Organizer and Sponsor may cancel Contest without prior notice in the case of force majeure causes that are beyond the reasonable control of Organizer and Sponsor, 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 and Sponsor 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.