ISECURION

VOLUME 1, MAY 2018

Infosec Newsletter

May, 2018

ISECURION TECHNOLOGY & CONSULTING PVT. LTD.

2nd Floor, #670, 6th Main Road, RBI Layout, Opp. Elita Promenade, J.P. Nagar 7th Phase, Bengaluru, Karnataka 560078

1. Windows Host Compute Service Shim Remote Code Execution Vulnerability:-

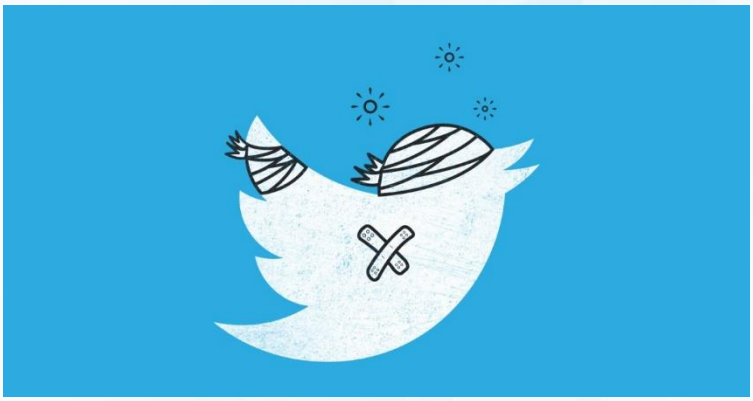
Windows Host Compute Service Shim (hcsshim) library fails to properly validate the input while importing container image which leads to remote code execution vulnerability. The attacker has to place the malicious code in a specially crafted container image, if an authenticated administrator imports, that will cause the container management service utilizing the Host Computer Shim library to execute malicious code on the host operating system.

Severity: Critical

CVE: CVE-2018-8115

To read more about this Click Here .

2. Bug Exposes Twitter Password in Plaintext



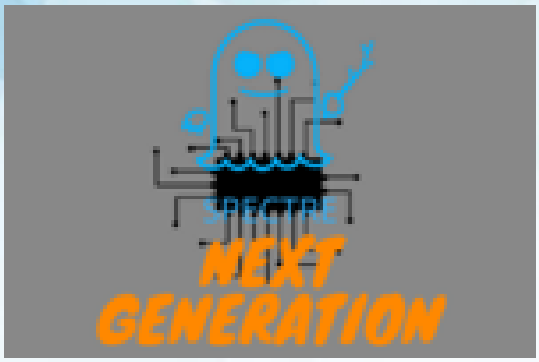
Twitter has more than 330 million users around the world. There was a software bug which resulted in logging of password to their internal log before it has been forwarded to the hashing process. The password has been left exposed into their internal network in plaintext format. Twitter has urged all its users to change the password of their account immediately and enable 2-factor-authentication. Which will prevent the account been hijacked by the attacker.

3. Rowhammer Attack and Hijack your android:-

It is Dubbed as **Glitch** it is a effective way to exploit 4 years old hacking technique called Rowhammer to hijack android mobile phone remotely. Rowhammer is a bug which resides in the dynamic random access memory (DRAM) chips, which repeatedly accessing a row of memory that can cause “bit flipping” in adjacent row, allowing anyone to change the value of contents stored in computer memory. A security team of VUSec Lab at Vrije University, Amsterdam demonstrated that Rowhammer technique can also exploit android smartphones. It took the team to host a website running JavaScript malicious code to remotely hack the android smartphone in 2 minutes without any software bugs. The malicious code is running within the web browser, it can spy on user’s browsing pattern or steal credentials. There is no software or patch that can fix the Rowhammer issue.

To read more about this Click Here.
Video PoC: YouTube.

4. New 8 Spectre-NG Found in Intel CPU:-

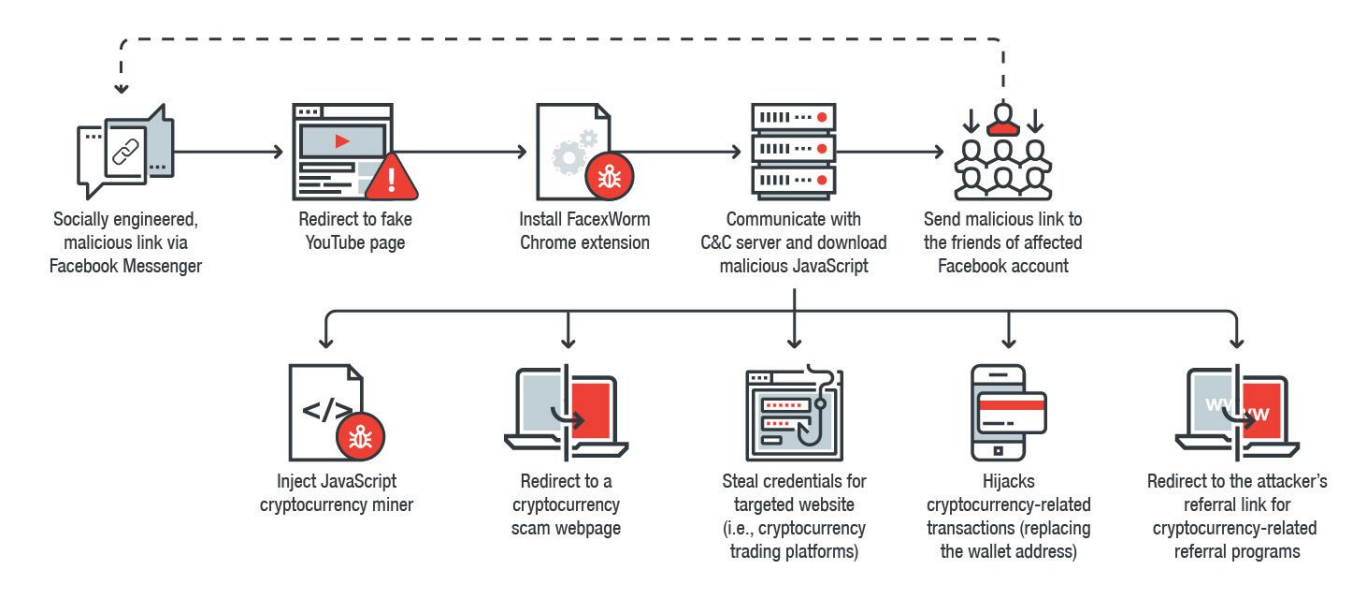


A security researchers has reported that the new 8 “Spectre-Class” vulnerabilities in Intel CPU which also affects small number of ARM processors and may impact AMD processors architecture as well. It has been dubbed as **Spectre-Next Generation** or **Spectre-NG** the partial details has been leaked at German computer magazine Heise, calming that Intel has classified four vulnerabilities as “high risk” and other four has “medium risk”. The newly discovered flaw allows attacker with access to a virtual machine to easily target the host system, which is potentially more threatening than the original Spectre vulnerability.

Intel has already acknowledged to release security patches in two shifts – one in May and other is currently scheduled for August.

To Read More about this: Click Here.

5. Facebook Cryptocurrency Mining Virus:-



If you receive any link of the video, even it looks exciting which has been sent by someone or maybe your friends on Facebook messenger – just don’t click without thinking. Security researchers from Trend Micro warning users of malicious Chrome extension which is spreading through Facebook and targeting users of cryptocurrency trading platform to steal their account credentials. The technique is dubbed as **FacexWorm,** which uses malicious extension to redirect users to cryptocurrency scams, injecting miners on web pages and redirecting users to cryptocurrency related referral programs.

To Read More about this: Click Here.

6. Microsoft Tuesday Patch May 2018:-

This month's update covers vulnerabilities in:-

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office
- Services and Web Apps
- ChakraCore
- Adobe Flash Player
- Microsoft Malware Protection Engine
- Microsoft Visual Studio

Software Patches Download List:-

- KB4093112 (OS Build 16299.371)
- KB4093118 (Monthly Rollup)
- KB4093108 (Security-only update)

7. Batch Overflow Bug in Etherium ERC20 token contracts (CVE-2018–10299):-

```
255   function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
256     uint cnt = _receivers.length;
257     uint256 amount = uint256(cnt) * _value;
258     require(cnt > 0 && cnt <= 20);
259     require(_value > 0 && balances[msg.sender] >= amount);
260
261     balances[msg.sender] = balances[msg.sender].sub(amount);
262     for (uint i = 0; i < cnt; i++) {
263         balances[_receivers[i]] = balances[_receivers[i]].add(_value);
264         Transfer(msg.sender, _receivers[i], _value);
265     }
266     return true;
267   }
268 }
```

In particular, on 4/22/2018, 03:28:52 a.m. UTC, PeckShield Inc. received an alert related to an unusual BEC token transaction. This transaction in particular someone trying to transfer extremely large amount of BEC token:

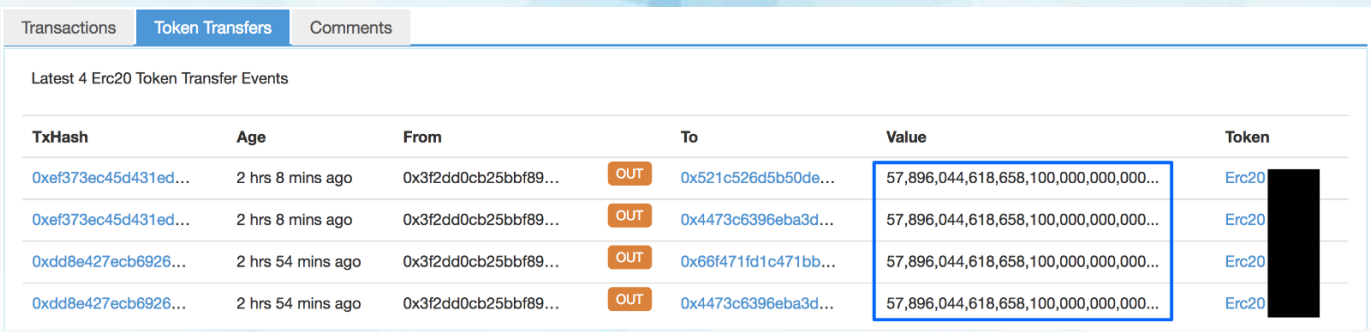
0x8000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000

Which consists of 63 0's, there were two large token transfers having same amount of tokens from BeautyChain contract to two different addresses. This prompted them to look into the smart code which further explained that the transfer comes from "in-the-wild" attack that exploits the vulnerability in the contract which has been dubbed as **batchOverflow.**

BatchOverflow is essentially a classic integer overflow issue. The vulnerability function exists in batchTransfer shown above in line 257. The *amount* local variable is calculated as product of *cnt* and *_value*. The second parameter i.e., *_value,* can be an arbitrary 256 bits integer like above token with

63 0's. By having two *_receivers* passed into *batchTransfer(),* with the extremely large *_value,* we can overflow *amount* and make it zero. With *amount* zeroed, an attacker can bypass the sanity checks in lines 258-259 and make the subtraction in line 261. The interesting part is shown in lines 262-265, the balance of two receiver would have added by the extremely large *_value* without costing a penny in the attacker's pocket!

They also found the vulnerability in dozen of ERC20 contracts which are vulnerable to batchOverflow. They also demonstrated by successfully transacted with one vulnerable contract with the proof-of-exploit provided below.



To Read More about this: Click Here.

8. Blacklisted IP Addresses of April 2018:-

- 212.92.115.117
- 217.219.25.19
- 188.253.40.139
- 107.17.3.28.179
- 60.3.144.233

9. Top Data Breaches of April 2018:-

- Dawson County
- Leominster Schools
- Ukraine Energy Ministry