ISECURION
YOUR SECURITY, OUR RESPONSIBILITY

VOLUME 5, SEPTEMBER 2018

Infosec Newsletter

September, 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. Unpatched Windows 0-day Vulnerability

A security researcher has publically disclosed a 0-day in Microsoft Windows operating system that could help a local use to obtain system privilege on the targeted system. The 0-day flaw has been confirmed working on fully patched 64-bit Windows 10 system. The vulnerbility resides in the Windows's task scheduler program and occurred due to erros in handling in Advanced Local procedure Call (ALPC) systems. The 0-day comes from a Twitter use with the online alias SandboxEscaper, also posted the proof-of-concept exploit in the github page.
Later, CERT/CC vulnerbility analyst Will Dormann verfiied the authencity of the 0-day bug, fully working on a fully-patched 640bit Widnows 10 system. The CVSS score for this vulnerbility is between 6.4 to 6.8. SandboxEscaper did no even notify Microsoft about the 0-day vulnerbility while leaving all the windows users vulnerbale to hackers.

To read more about this Click Here.

Poc exploit: GitHub.

2. MikroTik Router Eavesdropping Network Traffic

Top 20 Vulnerable Nations	Top attackers	List of PORTS Being eavesdropped
42376 Brazil/BR	5164 37.1.207.114	5837 21
40742 Russia/RU	1347 185.69.155.23	5832 143
22441 Indonesia/ID	1155 188.127.251.61	5784 110
21837 India/IN	420 5.9.183.69	4165 20
19331 Iran/IR	123 77.222.5445	2850 25
16543 Italy/IT	123 103.193.137.211	1328 23
14357 Poland/PL	79 24.255.37.1	1118 1500
14007 United States/US	26 45.76.8843	1095 8083
12898 Thailand/TH	16 206.255.37.1	993 3333
12720 Ukraine/UA		984 50001
11124 China/CN		982 8545
10842 Spain/ES		677 161
8758 South Africa/ZA		673 162
8621 Czech/CZ		355 3306
6869 Argentina/AR		282 80
6474 Colombia/CO		243 8080
6134 Cambodia/KH		237 8081
5512 Bangladesh/BD		230 8082
4857 Ecuador/EC		168 53
4162 Hungary/HU		167 2048

Chinese security researchers at Qihoo 360 Netlab have discovered more than 300,000 vulnerable MikroTik routers, which allows compromised device to enable socks4 proxy maliciously and eavesdrop on the target network traffic. The vulnerability CVE-2018-14847 Winbox Any Directory File Read in MikroTik routers that was found exploitable by CIA Vault 7 hacking tool called Chimay Red, along with MikroTik webfig remote code execution vulnerability. Winbox and Webfig are both RouterOS management components which uses communication ports TCP/8291, TCP/80 and TCP/8080. At present more than 7000 RouterOS device IPs have been compromised by the attacker and their network traffic has been forwarded to collecting IP addresses. The best way to fix this is to update their MikroTik RouterOS and check devices for HTTP proxy, Sock4 proxy and any network traffic capture function is exploited maliciously.

To read more about this Click Here.

3. Adobe Security Patches August 2018

- Adobe Acrobat and Reader (APSB18-29)
- Adobe Experience Manager (APSB18-26)
- Adobe Flash Player (APSB18-25)
- Adobe Creative Cloud Desktop Application (APSB18-32)
- Adobe Photoshop CC (APSB18-28)

To read more about this Click Here.

4. North Korean Spy charged by U.S. for WannaCry and Sony Pictures Hack

The U.S. Department of Justice has announced criminal charges against North Korean government spy for the connection with WannaCry ransomware attack in 2017 and Sony pictures Entertainment hack in 2014. The charges were brought up against Park Jin Hyok, who works for North Korean military intelligence agency Reconnaissance General Bureau (RGB). The Sony hack exposed more than 200GB of confidential data, including movie scripts, celebrity's phone number and also high-quality versions of 5 unreleased films. It has also wiped out 70 percent of the company computers and more than half of its servers, which was later published by WikiLeaks. WannaCry virus made havoc last year by crippling more than 300,000 hospitals, government agencies and other organization in 150 countries within three days.

To Read More about this: Click Here.

5. Microsoft Tuesday Patch September 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**
- **.NET Framework**
- **Microsoft.Data.OData**
- **ASP.NET**

Software Patches Download List:-

- ADV180022
- ADV180023
- CVE-2018-8315
- CVE-2018-8331
- CVE-2018-8336
- CVE-2018-8419
- CVE-2018-8424
- CVE-2018-8429
- CVE-2018-8430
- CVE-2018-8433
- CVE-2018-8434
- CVE-2018-8442
- CVE-2018-8443
- CVE-2018-8444
- CVE-2018-8445
- CVE-2018-8446
- CVE-2018-8452
- CVE-2018-8474

Known Issues:-

- 4457128
- 4457144
- 4458321

To Know More: Visit Here

6. British Airways Hacked

British Airways has confirmed that a data breach has exposed personal details and credit-card numbers of upto 380,000 customers and lasted more than two weeks. They have also released that customers who has book flights on its website (ba.com) and mobile app on 21st August 2018 to 5th September 2018 have been compromised. The airline have also advised the customers who made booking during that 15 days period have been affected and to contact their banks or credit card providers for recommended advice. The national Crime Agency has partnered with British Airways to assess the bets course of action for the data breach.

To Know More: Click Here

7. Tor Browser 0-day Exploit

Zerodium, the infamous exploit vendor recently shared a 0-day vulnerability that resides in NoScript plugin that comes pre-installed within Mozilla Firefox bundled in the Tor software. NoScript is a free browser plugin that blocks JavaScript, Java, Flash and other content on all websites by default. Zerodium concluded that NoScript versions 5.0.4 to 5.1.8.6 which is included in Tor Browser 7.5.6 can be bypassed to run any JavaScript file by changing its content-type header to JSON format. NoScript has fixed its 0-day flaw with the release of version 5.1.8.7. Tor browser has also released a new version of 8.0 which is not vulnerable to this flaw.

To Know More: Click Here.

8. WordPress PHP Code Execution

WordPress is one of the popular content management system used by world for blogging. Recently Sam Thomas, a security researcher from Secarma, has discovered a new exploiting technique that could allow hackers to trigger critical deserialization vulnerabilities in PHP programming language. PHP unserialization or object injection vulnerabilities which could allow an attackers to perform different kinds of attacks by supplying inputs to the unserialze PHP functions. Serialization is a process of converting data objects into plain strings and unserialze function help program recreate an object back from string. An attacker can even exploit this vulnerability using JPEG image, originally a Phar archive converted into valid JPEG by modifying its first 100 bytes. Once the image is uploaded on the target WordPress server, an attacker can use another function to call the same image, eventually executing arbitrary code when the program desterilizes the metadata.

To Know More: Click Here