ISECURION

VOLUME 2, JUNE 2018

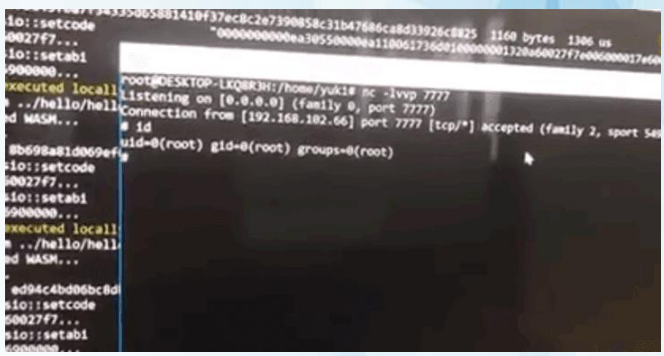
Infosec Newsletter

June, 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

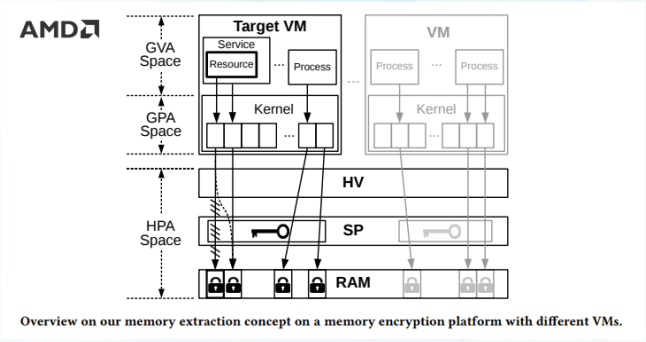
1. RCE Discovered in EOS Smart Contract System of Blockchain:-



EOS is and open source smart contract system that works just like Ethereum. It was discovered by Chinese security researcher at Qihoo 360, the functionality to parse contracts in nodes server is vulnerable to buffer out-of-bonds. To achieve remote code execution the attacker have to upload a malicious smart contract file known as WASM file written in Webassembly to the server. As the WASM file gets processed the malicious payload gets executed on the node server, which allows to take control of the supernode in EOS network, which collects transaction information. The attacker can take full of the supernode and can launch a cyber-attack or become a free miner.

To read more about this Click Here.

2. AMD's SEV Virtual Machine Encryption Bypassed by German Researcher



Overview on our memory extraction concept on a memory encryption platform with different VMs.

German security researcher claims that he has found a new practical attack against virtual machine protected by AMD's Secure Encrypted Virtualization (SEV) technology. During the test team where able to extract from the test server with entire 2GB memory data which includes data from another guest VM. Apache and Nginx web server's data extraction of memory at a speed of 79.4KB/sec and OpenSSH extraction speed to only 41.6KB/sec.

To read more about this Click Here.

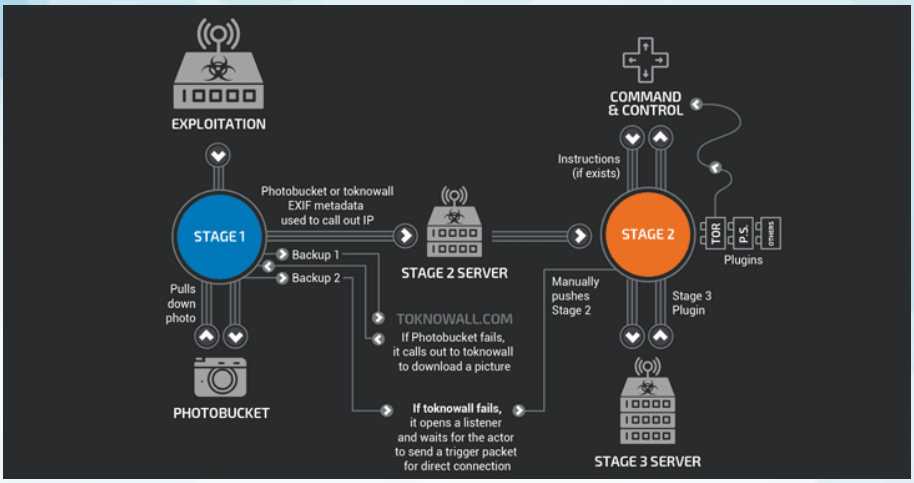
3. Z-Wave Downgrade Attack on IoT Devices:-

Z-Wave protocol is a wireless, radio frequency based communication technology that is used in the home automation devices to communicate with each other. It is designed to process remote control of appliances like lighting control, security systems, thermostats, windows, locks, swimming pools and garage door openers, up to a distance of 100 meters. The researcher found that the node info command which contains the security class is transferred unencrypted and unauthenticated, which allows attacker to intercept or broadcast malicious node commands without setting the security class.

To read more about this Click Here.

Video PoC: YouTube.

4. VPNFilter : Botnet army of 500000 hacked routers:-



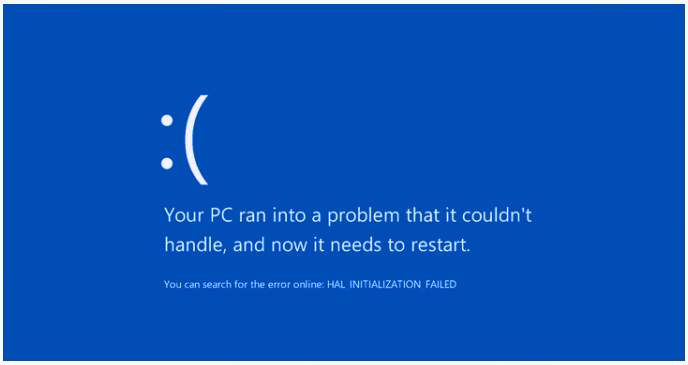
VPNFilter is a multi-stage, modular malware that can steal website credentials and monitor industrial controls or SCADA systems, such as electric grids, other infrastructure and factories. It communicates over Tor anonymizing network and even contains a kill switch for routers, where the malware can kill itself. The malware has infected over 500000 devices in 54 countries of small and home offices routers which includes Linksys, MikroTik, NETGEAR and TP-LINK.

It creates a directory "/var/run/vpnfilter" to hide its files on the infected devices. If you are already infected, reset the router and update the firmware to the latest update and if the router is still vulnerable after update, buy a new router.

It is recommended to put your router behind firewall and turn off administration until you require.

To Read More about this: Click Here.

5. How Ultrasonic and Sonic Signals can crash the Hard Disk?:-



The team of researchers from the University of Michigan and Zhejiang University demonstrated how sonic and ultrasonic signals which are inaudible to human can cause physical damage to hard drives just by playing a sound signals through a target computer's built in speakers or nearby speakers.

Modern HDD have a shock sensor to prevent it from getting damage they use shock-driven feedforward controllers that detects the movement and improve the position of the head while reading and writing. They also successfully demonstrate how an attacker can exploit the disk drive against the HDDs found in CCTV systems and desktop computers.

They have tested against different types of HDD which includes Seagate, Toshiba and Western Digital, which took 5-8 seconds to crash the Hard Disk. The Dell XPS 15 9550 laptop freezes at 45 seconds and 125 seconds to crash the laptop by using a ultrasonic signals.

To Read More about this: Click Here.

6. Microsoft Tuesday Patch June 2018:-

This month's update covers vulnerabilities in:-

- Internet Explorer
- Microsoft Edge
- Microsoft Windows
- Microsoft Office and Microsoft Office Service and Web Apps
- ChakraCore
- Adobe Flash Player

Software Patches Download List:-

- CVE-2018-3639 (Windows 10)
- CVE-2017-5715 CVE-2017-5754 CVE-2018-3639(Windows Server 2016)
- CVE-2018-3639 (Windows 8.1)
- CVE-2017-5715 CVE-2017-5754 CVE-2018-3639(Windows Server 2012 R2)
- CVE-2018-3639 (Windows RT 8.1)
- CVE-2018-3639 (Windows 7)
- CVE-2017-5715 CVE-2017-5754 CVE-2018-3639(Windows Server 2008 R2)
- CVE-2017-5715 CVE-2017-5754 CVE-2018-3639(Windows Server 2008)

Known Issues:-

- 4284880
- 4284819
- 4284835
- 4284826
- 4284867

To Know More: Click Here

7. Adobe Patches Actively Exploited Flash Player Zero-Day Exploit:-

It was discovered by several security firms. including ICEBRG, Qihoo 360 and Tencent that the Adobe player zero-day attacks have been targeting users in Middle East uses a specially crafter version of Excel spreadsheet.

The CVE-2018-5002, stack-based buffer overflow impacts version 29.0.0.171 can be exploited to execute arbitrary code on the target system. The vulnerability resides in the interpreter code of Flash Player, which fails to handle correctly the exception for try/catch statements.

The researcher explained that while processing try catch statement, it is impossible to execute the catch block, the attacker uses the getlocal, setlocal instruction in the catch block to read and write arbitrary addresses on the stack.

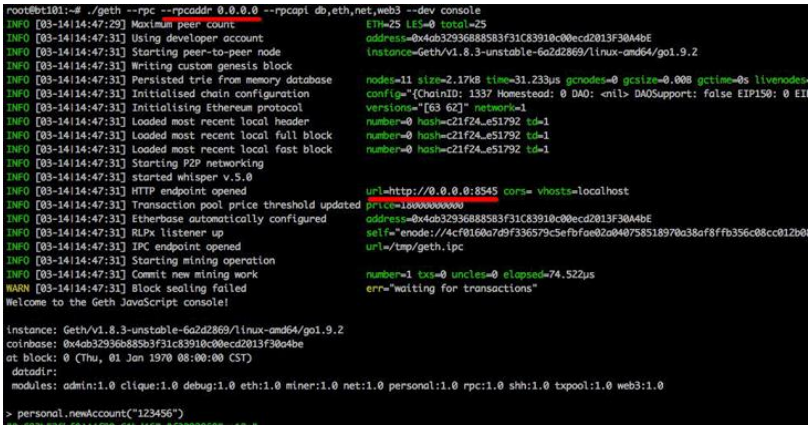
Beside this Adobe has also rolled security updates for Integer Overflow bug (CVE-2018-5000) and an Out-of-bounds (CVE-2018-5001) both leads to information disclosure.

It is highly recommended to update immediately the Adobe Flash Player to versions 30.0.0.113.

To Read More about this: Click Here.

Adobe Flash Player Patches Link: Click Here.

8. $20 Million Ethereum stolen from Insecurely Configured Clients:-



Qihoo 365 Netlab noticed that another cybercriminal group managed to steal a total 38642 Ether from the user by hijacking Ethereum wallets who had opened their JSON-RPC port 8545 to the outside world.

Geth is one of the top clients running Ethereum node and enabling JSON-RPC interface allowing anyone to access the Ethereum Blockchain and node facilities like send transactions to any account.

Attacker Ethereum address: 0x957cd4ff9b3894fc78b5134a8dc72b032ffbc464

By searching it on the internet you will find the similar type on incident happened, with the same account address used to steal from the insecurely configured Ethereum nodes.

9. Cryptocurrency crashed after Coinrail crypto exchange got hacked :-

The South Korean cryptocurrency exchange, Coinrail suffered a breach on Sunday losing 30 percentage of its cryptocurrency reserves. The exchange has yet not confirmed the estimated loss but the local news outlet Yonhap News reports stolen funds of approximately $37.2 million. Coinrail has traded over $2.48 million 24hrs before it got hacked. They claims 70 percentage of its cryptocurrency reserves are safe and been transferred to cold wallet and will resume services once the exchange service is stabilized.

Coinrail team might be able to recover 20 percent through the collaboration with other various cryptocurrency exchange desks, where the stolen funds has been moved. It has requested to exchanges to either freeze or recall the funds. The company is still investigating with the remaining 10 percent. During the investigation the wallet address of the attacker has been identified: 0xdf9191889649c442836ef55de5036a7b694115b6. The company has frozen the tokens that were stolen like NPER, DENT, TRX, KNC, JNT, STROM, B2B, Aston, also been affected by this hack and are frozen until further investigation.

The wallet named “Fake_phishing1432” received the coins from another wallet named “Fake_Phishing1431” before moving the coins to IDEX.