ISECURION
YOUR SECURITY, OUR RESPONSIBILITY

VOLUME 6, OCTOBER 2018

Infosec Newsletter

OCTOBER, 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. Pegasus spyware deployed in 45 countries

Citizen Lab revaled that one of the world's most dangerous Android and IPhone spyware have been found that it has been deployed against target across 45 countires for last two years. The Peagasus spyware is developed by NSO Group, an Israeli company capable for selling high-tech survelliance tools used for remotly cracking into iPhones and Android devices for intelligence agencies.
India is also in the list of countries targeted by Pegasus. In reponse to the Citizen Lab report, NSO spokesperson says that the company is working in full compilance with all conutries without breaking any laws.

To read more click here.

2. MikroTik Router Remote Code Execution

A security researcher from Teenable released a proof-of-concept (PoC) of RCE attack for an old directory traversal vulnerability. The vulnerability is identified as CVE-21018-14847, was rated as medium but now the severity is moved to critical as the new technique used to exploit this vulerbility on MikroTik routers allowiing attackers to remotly execute code on the affected devices to gain root shell.

The vulnerability allows attacker to remotly bypass authentication and read arbitrary files by modifying a request to change one byte related to session ID. MikroTik has rleased a patch for this vulnerability ans also asked user to update th RouterOS as soon as possible.

To read more about this Click Here.

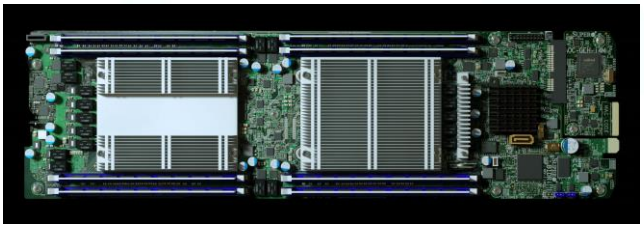
3. Adobe Security Patches August 2018

- Adobe Acrobat and Reader (APSB18-34)
- Adobe Flash Player (APSB18-31)
- Adobe ColdFusion (APSB18-33)
- Adobe Creative Cloud Desktop Application (APSB18-32)
- Adobe Photoshop CC (APSB18-28)

To read more about this Click Here.

4. China Hardware Spying on other Countries

According to a report published in Bloomberg, a tiny surveillance chip was found hidden inside the servers used by approx. 30 American companies which includes Apple and Amazon. The chip was inserted during the manufacturing process in China which is not even a part of the original design by U.S-based Company Super Micro. The chips is helping Chinese government to spy on American companies and their users.



Supermicro and Chinese officials have fully denied Bloomberg's report on the chip being implanted on the server motherboard to spy on other companies.

To Read More about this: Click Here.

5. Microsoft Tuesday Patch October 2018

This month's update covers vulnerabilities in:-

- **Internet Explorer**
- **Microsoft Edge**
- **Microsoft Windows**
- **Microsoft Office and Microsoft Office Services and Web Apps**
- **ChakraCore**
- **.NET Core**
- **PowerShell Core**
- **SQL Server Management Studio**
- **Microsoft Exchange Server**
- **Azure IoT Edge**
- **Hub Device Client SDK for Azure IoT**

Software Patches Download List:-

- ADV180026
- CVE-2010-3190
- CVE-2018-8292
- CVE-2018-8330
- CVE-2018-8427
- CVE-2018-8432
- CVE-2018-8472
- CVE-2018-8481
- CVE-2018-8482
- CVE-2018-8486
- CVE-2018-8493
- CVE-2018-8501
- CVE-2018-8503
- CVE-2018-8504
- CVE-2018-8506
- CVE-2018-8530
- CVE-2018-8532
- CVE-2018-8533

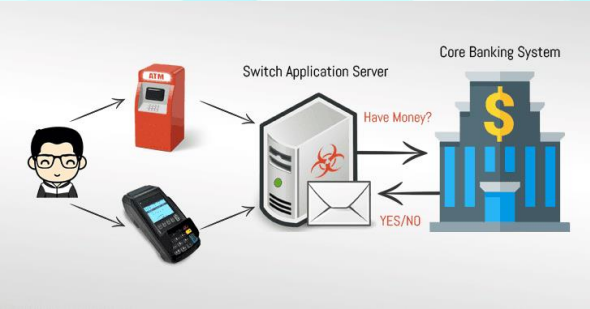
Known Issues:-

- 4459266
- 4462917
- 4462923

To Know More: Visit Here

6. Hacking Bank Servers to Spit out Cash from ATM

The hacking of bank servers to spit out cash from ATM is used by North Korean APT hacking group known as Hidden Cobra or Lazarus Group or Guardians of Peace which is also backed by the North Korean government to launch attacks against number of media organizations, aerospace, financial and critical infrastructure around the world.



The Hidden Cobra were managed to compromise the switch application server at different banks, where they had accounts. The malware installed on the compromised switch application server to intercept and modify the response to fool the ATM to spit out large number of cash without notifying the bank.The US-CERT had published advisory alerting users about the two different malwares – Remote Access Trojan (RAT) known as Joanap and Server Message Block (SMB) worm called as Brambul linked to Hidden Cobra.

To Know More: Click Here

7. Bitcoin Core Patches DDoS Attack Vulnerability

Bitcoin core development team has released an important patch to its underlying software for its Bitcoin Network. The DDoS vulnerability CVE-2018-17144 has been found on the Bitcoin Core Wallet software to crash any Bitcoin core nodes running software versions 0.14.0 to 0.16.2.

The DDoS attack on the BTC network would have costed miners 12.5 bitcoins which would be equivalent to $80,000 in order to successfully perform this attack.

To Know More: Click Here.

8. Western Digital's NAS Authentication Bypass

Security researches has found a vulnerability in Western Digital NAS designated as CVE-2018-17153, by simply including a cookie username=admin to the HTTP CGI request send to the device web interface, attacker can gain access to all the content on the NAS box.
The researcher has successfully verified the vulnerability in Western Digital model WDBCTL0020HWT running firmware version 2.30.172, but the vulnerability is not limited to the model, as most products of My Cloud series share the same vulnerability.

To Know More: Click Here

9. Ghost DNS : DNS Changer Botnet

Chinese security researcher have uncovered a widespread of ongoing malware that have hijacked over 100,000 home routers and modified their DNS settings to hack users with malicious web pages to steal bank details and login credentials. The GhostDNS scan the IP address for routers with default, no password or weak passwords to access the router's settings and modify the default DNS address controlled by the attackers.
The GhostDNS is targeting Brazil only has it has covered 87% total routers.
NetLab security researchers have recommended to disable remote administration, changing local IP address, and hardcoding trusted DNS server in the router operating system and to use a strong password for the login.

To Know More: Click Here