ISECURION
YOUR SECURITY, OUR RESPONSIBILITY

VOLUME 8, DECEMBER 2018

Infosec Newsletter

DECEMBER, 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. PhpMyAdmin Releases Critical Software Update

The developers of phpMyAdmin, which most widely used to manage MySQL database has released an update to its software for patching several critical vulnerabilites. PhpMyAdmin is an open-source management tool for MySQL databses and are widely used by webmasters to manage their databases for websites, including content management systems like WordPress, Drupal and etc. The newly discovered phpMyAdmin vulnerabilites are Local file inclusion (CVE-2018-19968), which allows remote attacker to read sensitive information from the server, Cross-Site Request Forgery (CSRF)(CVE-2018-19969), which could allow injection of sql query to rename the database, reset user passwords, manipulating data and etc., Cross-site Scripting (XSS) (CVE-2018-19970), allows malicious attacker to inject malicious code into the dashboard through a crafted database/table name.

To read more click here.

2. Adobe Flash 0-day in Microsoft Office

Security researcher have discovered a new 0-day vulnerability inside Adobe Flash Player, which is actively exploiting in the wild, part of a campaign appears to be attacking health care institution. The vulnerbility CVE-2018-15982 in Flash Player, if exploited allows an attacker to execute arbitrary code on the targeted systems and gain full control over the system. Maliciously carfted Microsoft Office documents contians embded Flash Active X contorl header that renders when target user opents it, causing exploitation of the flash player. The vulnerability impacts Flash Player version 31.0.0.153 and earlier for products Google Chrome, Microsoft Edge and Internet Explorer 11. The same exploiting technique was used in attacking Russia state healthcare clinic institution.

To read more about this Click Here.

3. Adobe Security Patches December 2018

- Adobe Flash Player (apsb18-44)
- Adobe Photoshop CC (apsb18-43)
- Adobe Flash Player (apsb18-39)

To read more about this Click Here.

4. Quora, 100 Million User Data Stolen

Quora, one of the most popular question and answer website suffered a massive data breach with unknown hacker gaining unauthorized access to the sensitive personal information of about 100 million users.

Adam D'Angelo, the chief executive officer and co-founder of Quora, said that the following information where included in the breach:

- Account information, such as names, email address, encrypted passwords and imported data from social networking sites.
- Public contents, like questions, answers, comments and up-votes.
- Non-public content, like answer requests, down-votes and direct messages.

Quora have stored salted and hashed passwords to prevent it from cracking and also logged out all compromised users from their session and forced them to reset their password.

To Read More about this: Click Here.

5. Microsoft Tuesday Patch December 2018

This month's update covers vulnerabilities in:-

- **Adobe Flash Player**
- **Internet Explorer**
- **Microsoft Edge**
- **Microsoft Windows**
- **Microsoft Office and Microsoft Office Services and Web Apps**
- **ChakraCore**
- **.NET Framework**
- **Microsoft Dynamics NAV**
- **Microsoft Exchange Server**
- **Microsoft Visual Studio**
- **Windows Azure Pack (WAP)**

Software Patches Download List:-

- CVE-2018-8477
- CVE-2018-8514
- CVE-2018-8580
- CVE-2018-8595
- CVE-2018-8596
- CVE-2018-8598
- CVE-2018-8616
- CVE-2018-8621
- CVE-2018-8622
- CVE-2018-8627
- CVE-2018-8637
- CVE-2018-8638

Known Issues:-

- 4471321
- 4471327
- 4471329
- 4471324
- 4471318

To Know More: Visit Here

6. Marriott International Data Breach

The largest hotel chain Marriott International suffered a data breach on September 2018, an unknown hacker compromised the guest reservation database from Starwood hotels and took about 500 million guests personal data. Marriott discovered the data breach on September 8, 2018 received an alert from internal security tool that their guest reservation database was attempted to access. The database contains information about names, mailing addresses, phone number, email addresses, passport numbers, date of birth, genders, arrival and departure, reservation date and communication preferences. The stolen data also includes payment card numbers with expiration dates but according to Marriott they have encrypted the card numbers using Advanced Standard encryption (AES-128).

To Know More: Click Here

7. Dell Resets All Customers Passwords after Security Breach

Dell disclosed that its online electronics marketplace experienced a "cybersecurity incident" this month when an unknown group of hackers infiltrated its internal network. On November 9, Dell detected unauthorized activity on its network attempting to steal customer information, including names, email addresses and hashed passwords. On investigation Dell found on conclusive evidence that the hackers succeeded to extract any critical information, but as a countermeasure Dell has reset passwords of all accounts on Dell.com irrespective of the data stolen.

To Know More: Click Here.

8. Uber Fined $1.1 Million over 2016 Data Breach

British and Dutch data protection regulators hit the Uber, a ride sharing company with total fine of $1,170,892 (~ 1.1 million) for failing to protecct its customers personal information during a 2016 cyber attack. Uber had suffered a massive data breach in October 2016, which includes names, email addresses and phone number of 57 million Uber riders nad drivers with driving license numbers of around 600,000 drivers. ICO also confirmed that the attackers were able to compromise Uber's cloud-based storage system using a process by which compromised username and password pairs are injected into website until they are matched to an existing account. After 12 months after the attack Uber started monitoring affected riders and drivers accounts for fraud.

To Know More: Click Here

9. Google+ to Shut down Early After New API Flaws

Google recently revealed that Google+ suffered another massive data breach, forcing Google+ to shut down earlier than its actual scheduled date i.e., in April 2019 instead of August 2019. Google said that it has discovered another critical vulnerability in one of Google+'s API's that could have allowed developers to steal sensitive information on 52.5 million users, including their name, email address, occupation and age. Google also said that it has not found any evidence that the vulnerability has been exploited, also assured that its users that no passwords, financial data, national identification numbers or any sensitive data were left exposed by the API bug.

To Know More: Click Here

10. SNDBOX : AI Powered Automated Malware Analysis Platform

Israeli cyber security and malware researcher at Black Hat conference launch a machine learning and artificial intelligence-powered malware research platform that motive is to help users identify unknown malware samples before the strike. It is known as SNDBOX, the free online automated malware analysis system allows anyone to upload a file and access its static, dynamic and network analysis in graphical interface. It not only analysis the file but also analysis the network activity by intercepting DNS requests originating from the infected virtual machine while monitoring. Moreover, users can download the entire report for nay submitted malware sample, its PCAP file, as well as sample file itself.

To Know More: Click Here