ISECURION
YOUR SECURITY, OUR RESPONSIBILITY

VOLUME 7, NOVEMBER 2018

Infosec Newsletter

NOVEMBER, 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. WordPress Design Flaw to RCE in WooCommerce

The vulnerability was automatically detected by the security analysis solution RIPS in WooCommerce code within 2 minutes. The vulnerability allows any shop manager to delete a certain files on the server and take over any administrator account. The "shop_manager" roles in the wordpress is assigned with "edit_users" capability so that they are allowed to edit customer accounts of the store. The user roles are independent of the plugin and will exist even if the plugin is inactive. The file deletion vulnerability occurred in the logging feature of WooCommerce. Logs are stored as .log files in wp-content directory of WordPress. When a shop manager wants to delete a log file, he submits it's filename as a GET parameter.

To read more click here.

2. Bluetooth Chip RCE Vulnerabilities

An Israeli security firm Armis, the vulnerability exist in Bluetooth Low Energy Stack chips made by Texas Instruments (TI), which is used by Cisco, Aruba and Meraki in their enterprise line of produtcs. The Texas Instruments (TI) chips CC2640 and CC 2650, when more traffic is send to a BLE chip it causes memory corruption, commonly known as buffer overflow attack, allowing attacker to run a malicious code on the affected device identified as CVE-2018-16986. The second vulnerability identified as CVE-2018-7080 in cc2642R2, CC2640R2, CC2640, CC2650, CC 2540 and CC 2541 TI chips. The vulnerability issue is with the firmware update feaure in the BLE chips called Over the Air firmware Download (OAD). The access point share a common OAD password which can be obatined by sniffing legitimate update or by reverse engineering BLE firmware, an attacker can deliver a malcious update to the target point and rewrite its operating system, gaining full contorl over the device.

To read more about this Click Here.

3. Adobe Security Patches August 2018

- Adobe Acrobat and Reader (apsb18-40)
- Adobe Technical Communication Suite (apsb18-38)
- Adobe Framemaker (apsb18-37)
- Adobe Experience Manager (apsb18-36)
- Adobe Digital Editions (apsb18-27)
- Adobe Flash Player (apsb18-35)
- Adobe Acrobat and Reader (apsb18-30)

To read more about this Click Here.

4. VirtualBox Zero-Day Exploit

An independent security researcher, Sergey Zelenyuk published a technical details of the zero-day flaw on GitHub, which affects all the current versions (5.2.20 and prior) of VirtualBox software and is present in default Virtual Machine configuration. The vulnerability allows an attacker or a malicious program with root or administrative rights in the guest

OS to escape and execute arbitrary code in the application layer pf the host OS. The vulnerability occurs due to memory corruption issues and affects Intel PRO/1000 MT Desktop (82540EM) network card (E1000) when the network mode is set to NAT (Network Address Translation).

To Read More about this: Click Here.

5. Microsoft Tuesday Patch November 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**
- **Skype for Business**
- **Azure App Service on Azure Stack**
- **Team Foundation Server**
- **Microsoft Dynamics 365 (on-premises) version 8**
- **PowerShell Core**
- **Microsoft.PowerShell.Archive 1.2.2.0**

Software Patches Download List:-

- ADV180025
- CVE-2018-8407
- CVE-2018-8408
- CVE-2018-8454
- CVE-2018-8545
- CVE-2018-8558
- CVE-2018-8563
- CVE-2018-8565
- CVE-2018-8566
- CVE-2018-8573
- CVE-2018-8578
- CVE-2018-8579
- CVE-2018-8581
- CVE-2018-8592

Known Issues:-

- 4467691
- 4467696
- 4467686
- 4467702
- 4467107

To Know More: Visit Here

6. TRITON ICS Malware

Cybersecurity firm FireEye discovered evidence of a Russian-owned TRITON malware that caused some industrial systems to unexpectedly shutdown last year, including petrochemical plant in Saudi Arabia. TRITON is also known as Trisis, is a piece of ICS malware designed to target Triconex Safety Instrumented System (SIS) controllers made by Schneider Electric which is often used in oil and gas facilities.
Moscow-based lab Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM) helped attackers as it will be impossible to create such a malware without the necessary knowledge of Industrial Control Systems (ICS). An IP address 87.245.143.140 registered to CNIIHM has been employed for monitoring TRITON network reconnaissance and malicious activity.

To Know More: Click Here

7. Privilege Escalation Flaw Affects Linux Distribution

An Indian security researcher Narendra Shinde has discovered a flaw in X.Org Server package that affects most of the linux distributions. Xorg X server is a popular open-source implementation of the X11 system (display server) that offers a graphical environment to a wide range of hardware and OS platforms. It is used to manage graphical displays between client and user applications.

The Vulnerability is tracked as CVE-2018014665, which can be exploited by a local attacker on the terminal or via SSH to elevate their privileges on a target system. X.Org have released a security patch in address to the issue.

To Know More: Click Here.

8. Abusing Microsoft Office Online Video

Security researcher has revealed an unpatched logical flaw in Microsoft Office 2016 and older versions that could allow attackers to embed malicious code inside the word document, tricking users into malware on their computer. A word doc file (.docx) are zip packages of its media and configuration files which are easily accessible. The configuration file called “document.xml” used by the word contains the generated embedded-video code, can be manipulated to replace the video iFrame code with any HTML or javascript code that would run in the background. An attacker can exploit the bug by replacing the Youtube video with any malicious code that gets executed.

To Know More: Click Here

9. StatCounter Analytics Hijacked to Steal Bitcoins from Cryptocurrency Users

ESET malware researcher Matthieu Faou has spotted malicious JavaScript code on upto 700,000 websites that were bundled with the traffic tracking code from a leading web analytics platform StatCounter. After the code analysis of the researcher found that hackers managed to compromise StatCounter and replace the tracking script with malicious JavaScript code designed to target cryptocurrency exchange customers. The script only gets activated when it finds a specific Uniform Resource Identifier (URI) “myaccount/withdraw/BTC”.

To Know More: Click Here