InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Microsoft Updates Patchs Critical Flaws in Windows
2. Parts of Wikipedia Offline after attack
3. NetCAT, Remotely steals data from Intel CPUs
4. Vulnerabilities in PHP patched
5. New SIM Card Flaw Lets Hackers Hijack Any Phone Just By Sending SMS
6. D-Link and Comba Wi-Fi Routers Leak Their Passwords in Plaintext
7. New 'Joker' Malware Infecting 24 Android Apps

15/09/2019

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, ebay, eset, bugcrowd, under armour, coinbase, CCM, etc have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

1. Microsoft Updates Patch Critical Flaws in Windows

Description	
Microsoft has patched a total of 79 security vulnerabilities. These include elevation of privilege vulnerability residing in Windows Text Service Framework, Windows Operating System and in windows Log File System Driver. Microsoft has also patched vulnerabilities in its Remote Desktop Client application that enables a malicious RDP server to compromise the client's computer. Other patches include the way Windows OS processes .LNK shortcut files, an update for android app 'Yammer' and in various Microsoft's products including Chakra Script Engine, VBScript, VBScript, SharePoint server, Scripting Engine. Azure DevOps, Team Foundation Server among others.	
Source	https://thehackernews.com/2019/09/microsoft-windows-update.html
Recommendation	Install new windows updates

2. Parts of Wikipedia Offline after attack

Description	
Wikipedia went offline in several countries after the server of the Wikimedia Foundation, which hosts the site, faced a massive Distributed Denial Of Service Attack. DDoS attack often involves large number of requests being sent to the server slowing down services and thus as in this case knocking them offline.	
Source	https://gadgets.ndtv.com/internet/news/wikipedia-malicious-ddos-attack-september-7-wikimedia-statement-2097224
Infected Industry	Wikimedia Servers

3. NetCAT, Remotely steals data from Intel CPUs

Description	
Network Cache Attack (NetCAT), a network based side-channel vulnerability has been discovered by security researchers from the Vrije University in Amsterdam. It could allow attackers to detect sensitive data like SSH password from Intel's CPU cache. This vulnerability lies in Intel's Data-Direct I/O, a performance optimization feature which helps network devices and other devices access to the CPU cache. This attack works by sending specially crafted network packets to a targeted computer that has Remote Direct Memory Access (RDMA) feature enabled. This allows attackers to spy on remote server-side peripherals such as network cards and observe the timing difference between network packets that is served from the remote processor's cache vs a packet served from memory. Then it performs a keystroke timing analysis to recover words typed by a victim using a machine learning algorithm against the time information.	
Source	https://www.cs.vu.nl/~herbertb/download/papers/netcat_sp20.pdf
Infected Technology	Intel
Recommendation	Do not give access to network devices from untrusted networks. Disable RDMA, DDIO.

4. Vulnerabilities in PHP patched

Description	
PHP released its latest patch where it updated several high-severity vulnerabilities in its core and bundled libraries. The most critical of which were arbitrary code execution. The failed attempts of this exploitation could result in DDoS attacks. Other patched flaws affect curl extension, Exif function, FastCGI Process Manager (FPM), Opcache feature, and more.	
Source	https://www.php.net/ChangeLog-7.php#7.3.9
Infected Technology	PHP
Recommendation	Update to the latest version of PHP.

5. New SIM Card Flaw Lets Hackers Hijack Any Phone Just By Sending SMS

Description	
The existence of new and previously undetected critical vulnerability in SIM cards-dubbed as “SimJacker”- was revealed. This Vulnerability could allow remote attackers to compromise targeted mobile phones and spy on victims just by sending an SMS. The SimJacker Vulnerability can be exploited using a GSM modem to retrieve IMEI information, spying victims surrounding, spreading malware, sending fake messages on behalf of victim, performing DOS attacks by disabling the SIM card, retrieving information. The user is completely unaware that they received the attack. Simjacker represents a clear danger to the mobile operators and subscribers.	
Source	https://simjacker.com
Infected Technology	SIM Cards

6. D-Link and Comba Wi-Fi Routers Leak Their Passwords in Plaintext

Description	
A total of five vulnerabilities - two D-link DSL modem and three in multiple Comba Telecom WiFi devices- has been discovered. These vulnerabilities could potentially allow attacker to change your device setting,extract sensitive information, perform MitM attacks, redirect you to phishing or malicious sites. The vulnerabilities in D-link Wifi Router allow anyone to access file that contains login password in plaintext. And the vulnerabilities in Comba WiFi Router affects in leaking MD5 hash passwords and credentials stored in SQLite database	
Source	https://thehackernews.com/2019/09/router-password-hacking.html
Infected Technology	D-Link, Comba Wi-Fi Routers
Recommendation	Patch the updates as soon as they are available.

7. New 'Joker' Malware Infecting 24 Android Apps

Description	
A new malware called “Joker” is infecting Android apps and can steal money from your account by presenting itself as a premium subscription. This malware is designed to silently sign users up for subscription services. This malware has infected 24 apps on the Google Play Store, some of the apps are: Age Face, Beach Camera, Cute Camera, Climate SMS, Great VPN, etc.	
Source	https://lifehacker.com/uninstall-these-24-android-apps-infected-with-new-joker-1837979754
Infected Technology	Android
Recommendation	Do not install suspicious apps.

For any queries/recommendations:

Contact us: whois@cryptogennepal.com