InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Cisco Router IOS Critical Flaws
2. Nodersok fileless malware infects Microsoft devices
3. Zero-day vulnerability in internet explorer RCE
4. Simjacker: SIM Cards Vulnerability
5. 1-Click iPhone and Android Exploits target Tebetan Users via WhatsApp

29/09/2019

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. Cisco Router IOS Critical Flaws

Description

Cisco recently released patches for 29 bugs impacting its 800 and 1000 series routers and 13 of the vulnerabilities has a CVSS severity score of 9.9. Under the list of vulnerabilities there is Denial-of-Service attacks and command injection bugs. The Cisco's IOS software on the vulnerable series of routers with "Guest OS" can allow attacker to gain unauthorized access to the Guest OS as root user.

Source	https://threatpost.com/cisco-high-severity-bugs-2/148706/
Infected Technology	Cisco 800 and 1000 series routers
Recommendation	Patch your applications;
CVE ID	CVE-2019-12650, CVE-2019-12651, CVE-2019-12648, CVE-2019-12653, CVE-2019-12649, CVE-2019-12620, CVE-2019-12619

2. Microsoft: Nodersok & Divergent fileless malware

Description

Malware dubbed Nodersok and Divergent have been found infecting thousands of computers worldwide. The malwares are operating as fileless and it leverages the built-in system utilities and third-party tools to extend its functionality.

Source	https://www.zdnet.com/article/microsoft-new-nodersok-malware-has-infected-thousands-of-pcs/
Infected Technology	Microsoft Windows
Recommendation	Enable and update Windows Defender

3. Zero-day vulnerability in internet explorer RCE and Windows defender

Description	
The Remote Code Execution flaw found on the internet explorer can enable an attacker who has successfully exploited it to gain the same user rights as the current user. An out-of-band security update was sent by Microsoft to address these vulnerabilities.	
Source	https://threatpost.com/microsoft-internet-explorer-zero-day-flaw-addressed-in-out-of-band-security-update/148584/
Infected Technology	Microsoft Internet Explorer; Microsoft Defender
Recommendation	Apply the available patch provided by Microsoft
CVE ID	CVE-2019-1367 & CVE-2019-1255

4. Simjacker: More SIM Cards Vulnerability

Description	
The simjacker vulnerability has been found actively exploited and remotely compromised targeted phones by sending specially crafted SMS to the target's phone number. The vulnerability addressed with the simjacker resided in the dynamic SIM toolkit, called S@T Browser. Now, researchers have revealed in another SIM toolkit called Wireless Internet Browser (WIB).	
Source	https://simjacker.com/
Infected Technology	Subscriber Identification Module (SIM) Card

5. 1-Click iPhone and Android Exploits target Tibetan Users via WhatsApp

Description
A new sophisticated attack running a mobile hacking campaign targeting various Tibetan groups with one-click exploit on iOS and Android devices. The attack named *Poison Carp* sends a tailored malicious web links to its target over WhatsApp and after they opened, exploited web browser and Privilege escalation vulnerabilities to install spyware on iOS and Android devices.

Source	https://thehackernews.com/2019/09/iphone-android-hacking-tibet.html
Infected Technology	WhatsApp for iOS and Android
Recommendation	Keep your iOS and Android devices Up to date

For any queries/recommendations:

Contact us: whois@cryptogennepal.com