InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. GhostCat Flaw Found In All Version of Apache Tomcat
2. New Wi-Fi Encryption Vulnerability Affects Over A Billion Devices
3. New LTE Network Flaw Could Let Attackers Impersonate 4G Mobile Users
4. Chrome Browser Zero-Day Bug Under Attack
5. New Open SMPTD RCE Flaw Affects Linux and Open BSD Email Server

03/02/2020

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. Ghost Cat Flaw Found In All Version Of Apache Tomcat

Description	
It has been found that all versions (9.x/8.x/7.x/6.x) of the Apache Tomcat were vulnerable to the GhostCat flaw. A GhostCat flaw resides in tha Apache JServ Protocol (AJP) of Apache Tomcat software that arises due to improper handling of an attribute. This flaw could be exploited in default configuration which lead to file read and inclusion. The flaw could let unauthenticated, remote attackers read content of any file on a vulnerable web server and obtain sensitive configuration files or source code, or execute arbitrary code if the server allows file upload.	
Source	https://thehackernews.com/2020/02/ghostcat-new-high-risk-vulnerability.html
Infected Technology	Apache Tomcat
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2020-1938

2. New Wi-Fi Encryption Vulnerability Affects Over A Billion Devices

Description	
A new high-severity hardware vulnerability was found in the widely-used Wi-Fi chips manufactured by Broadcom and Cypress affecting billion devices, including smartphones, tablets, laptops, routers, and IoT gadgets. The bug stems from the use of an all-zero encryption key in chips made by Broadcom and Cypress, which results in data decryption. the flaw could let nearby remote attackers intercept and decrypt some wireless network packets transmitted over-the-air by a vulnerable device.	
Source	https://threatpost.com/billions-of-devices-wifi-encryption-hack/153267/
Infected Technology	Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (RedMi), Asus and Huawei.
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2019-15126

3. New LTE Network Flaw Could Let Attackers Impersonate 4G Mobile Users

Description	
A new LTE Network Flaw -Impersonate Attack is affecting 4G mobile technologies has been identified in IoT devices. The impersonation attack — named "**IMPersonation Attacks in 4G NeTworks**" (or IMP4GT) — exploits the mutual authentication method used by the mobile phone and the network's base station to verify their respective identities to manipulate data packets in transit. The IMP4GT attacks exploit the missing integrity protection for user data, and a reflection mechanism of the IP stack mobile operating system which allows to inject arbitrary packets and to decrypt packets. This security flaws in 4G LTE and 5G networks that could potentially allow hackers to impersonate users on the network and even sign up for paid subscriptions on their behalf.	
Source	https://thehackernews.com/2020/02/lte-network-4g-vulnerability.html
Infected Industry	Smart phones, Tablets and IoT devices with LTE Networks

4. Chrome Browser Zero-Day Bug Under Attack

Description	
The Chrome web browser was facing a zero-day bug being actively exploited in the wild. The flaw affects versions of Chrome running on the Windows, mac OS and Linux platforms. The zero-day bug tied to memory corruptions found inside the Chrome browser's open-source JavaScript and Web Assembly engine, called V8. The memory corruption vulnerabilities occur when memory is altered without explicit data assignments triggering programming errors, which enable an adversary to execute arbitrary code on targeted devices.	
Source	https://threatpost.com/google-patches-chrome-browser-zero-day-bug-under-attack/153216/
Infected Industry	Google Chrome
Recommendation	Update the latest patch released.
CVE_ID	CVE-2020-6418

5. New Open SMPTD RCE Flaw Affects Linux and Open BSD Email Server

Description	
Open SMTPD has been found vulnerable to a critical vulnerability that could allow remote attackers to take complete control over email servers running BSD or Linux operating systems. Open SMTPD comes pre-installed on many UNIX-based systems. The new Open SMTPD flaw can be exploited by a local or remote attacker in two ways by sending specially crafted SMTP messages, one works in the default configuration, and the second leverages email bounce mechanism.	
Source	https://thehackernews.com/2020/02/opensmtpd-email-vulnerability.html
Infected Technology	Linux , Open BSD Email Server
Recommendation	Update the latest patch released.
CVE_ID	CVE-2020-8794

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**