InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Smominru Botnet hacked over 90,000 computers
2. PhpMyAdmin Zero-day affects all versions
3. Thousands of Google Calendars leaking private information
4. Vulnerabilities in PHP patched
5. Flaws found in Popular Routers and NAS Brands
6. Ad Fraud Scheme on Popular Ad Blocker Extensions
7. New Critical Flaws on Google's Chrome Browser

22/09/2019

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. Smominru Botnet hacked over 90,000 computers

Description	
An infamous cryptocurrency-mining and credential-stealing botnet named Smominru, has become one of the rapidly spreading computer viruses that is now infecting over 90,000 machines each month around the world. Only last month, more than 4,900 networks were infected by the worm. The botnet was found gaining access to vulnerable systems by brute forcing weak credentials. When smominru gets the access, it installs a Trojan module and a cryptocurrency miner and then it propagates inside the network.	
Source	https://www.guardicore.com/2019/09/smominru-botnet-attack-breaches-windows-machines-using-eternalblue-exploit
Infected Technology	Vulnerable Applications facing the Internet
Recommendation	Patch your applications; stronger passwords are highly recommended

2. phpMyAdmin Zero-Day affects all versions

Description	
A very critical bug was detected on one of the most popular applications for managing the MySQL and MariaDB databases. The vulnerability claims to be a cross-site request forgery (CSRF) flaw, also known as XSRF, a well-known attack wherein attackers trick authenticated users into executing an unwanted action. This vulnerability allows attacker to delete any server configured in the setup page of PhpMyAdmin panel.	
Source	https://nakedsecurity.sophos.com/2019/09/20/server-squashing-zero-day-published-for-phpmyadmin-tool/
Infected Technology	phpmyadmin
Recommendation	Apply Updates that are available

3. Thousands of Google Calendars Leaking private information

Description	
Security researcher claims to have found more than 200 calendars leaking information that should be private. The issue is related to the public visibility set on the google calendar by the users. Google fails to send any notification to the users warning them about the visibility of their calendar.	
Source	https://securityaffairs.co/wordpress/91393/digital-id/google-calendar-data-leak.html
Infected Technology	Google Calendars
Recommendation	Check your google settings and check if you're exposing all your events and business activities on the Internet accessible to anyone

4. Flaws Found in Popular Router and NAS brands

Description	
Security researchers have discovered a total of 125 different security vulnerabilities across 13 small office/home office (SOHO) routers and NAS devices that have the potential to affect millions of users. The vulnerabilities ranged from XSS, CSRF, Buffer Overflow, Command Injection, etc.	
Source	https://www.techradar.com/news/flaws-discovered-in-popular-router-and-nas-brands
Infected Technology	Buffalo, Synology, TerraMaster, Zyxel, Drobo, ASUS and its subsidiary Asustor, Seagate, QNAP, Lenovo, Netgear, Xiaomi and Zioncom (TOTOLINK)
Recommendation	Update any firmware that is available

5. Ad Fraud Scheme on Popular Ad Blocker extension

Description	
AdBlock and uBlock Origin, two popular Google Chrome Extensions have been caught stuffing cookies in the web browser of millions of users to generate affiliate income from referral schemes fraudulently. Cookie Stuffing, also known as Cookie Dropping, is one of the most popular types of fraud schemes in which a website or a browser extension drops handfuls affiliate cookies into users' web browser without their permission or knowledge. These affiliate tracking cookies then keep track of users' browsing activities and, if they make online purchases, the cookie stuffers claim commissions for sales that they had no part in making, potentially stealing the credit for someone else's attribution fraudulently.	
Source	https://www.techradar.com/news/flaws-discovered-in-popular-router-and-nas-brands
Infected Technology	Ad Blockers
Recommendation	Remove these two Extensions; AdBlock & uBlock Origin

6. New Critical Flaws on Google Chrome Browser

Description	
Google released an urgent software update for its chrome web browser on all platforms (Linux, Mac and Windows). The security patch contains 1 critical and 3 high-risk security vulnerabilities, one of the most severe one could allow remote hackers to take control of an affected system.	
Source	https://thehackernews.com/2019/09/google-chrome-update.html
Infected Technology	Google's Chrome Browser
Recommendation	Patch your google chrome browser

For any queries/recommendations:

Contact us: whois@cryptogennepal.com