InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Linux VPN Hijacking
2. Avast and AVG browser extensions user data
3. GoAhead web Server Critical Flaw
4. Facebook Ads Manager Targeted By New Info-Stealing Trojan
5. StrandHogg Vulnerability

09/12/2019

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. **Linux VPN Hijacking**

Description	
A new vulnerability in Linux and Unix like operating system has been recently discovered which allows remote 'network adjacent attackers' to spy and tamper with encrypted VPN connections. This vulnerability can be exploited by an attacker just by sending unsolicited network packets to a targeted device and observing replies, even if they are encrypted. The vulnerabilities allows attackers to determine the virtual IP address assigned by the VPN server or determine the exact seq and ack numbers by counting encrypted packets or examining their size and even inject data into the TCP stream and hijack connections.	
Source	https://thehackernews.com/2019/12/linux-vpn-hacking.html
Infected Technology	Linux OS
Recommendation	Apply patch updates as soon as it is available
CVE_ID	CVE-2019-14899

2. Avast and AVG browser extension collecting user data

Description	
Security researcher Wladmir Palant discovered these malicious behaviour of Avast and AVG extensions. These software automatically installs their respective add-ons on the users' browsers. These extensions have been designed to warn users when they visit a malicious or phishing website. Collected data includes full url of the page the user is on, including query part and anchor data, page title, a value that tells whether the user visited the page before, country code, browser name and its exact version, operating system and its exact version number	
Source	https://thehackernews.com/2019/12/avast-and-avg-browser-plugins.html
Infected Technology	Avast & AVG
Recommendation	Do not use Avast & AVG anti-virus on personal conputers

3. GoAhead Web Server Critical Flaw

Description
GoAhead is an application embedded in millions of internet connected smart devices. One of the vulnerability that has been discovered is a critical code execution flaw that can be exploited by attackers to execute malicious code on vulnerable devices and take control over them. According to the researchers at Cisco Talos, while processing a specially crafted HTTP request, an attacker exploiting the vulnerability can cause use-after-free condition on the server and corrupt heap structures, leading to code execution attacks. Another vulnerability also resides in the same component of the GoAhead Web Server and can be exploited in the same way, but this one leads to denial-of-service attacks.

Source	https://securityaffairs.co/wordpress/94692/hacking/goahead-rce.html
Infected Technology	GoAhead Web Server v5.0.1 v4.1.1and v3.6.5
Recommendation	Update the patch when available
CVE_ID	CVE-2019-5096 CVE-2019-5097

4. Facebook Ads manager Targeted By New Info-Stealing Trojan

Description	
Facebook ads are being targeted by a new trojan which could allow a malicious actor to access not only regular advertisements but the growing number of political spots being posted to social media giant.The trojan called Socelars , is distributed through a fake PDF editing app named PDFreader attempts to mine data from Facebook ads was turned up.Once activated the Trojan attempts to steal Facebook session cookies from Chrome and Firefox through SQLite database and then use them to connect to different Facebook URLs.	
Source	https://www.bleepingcomputer.com/news/security/facebook-ads-manager-targeted-by-new-info-stealing-trojan/
Infected Technology	Social Site (Facebook Ads)

5. StrandHogg Vulnerability

Description	
Researchers have discovered a new Android Vulnerability that could allow malware to pose as popular apps and ask for various permissions, potentially allowing hackers to listen in on users , take photos, read and send SMS messages , and basically take over various functions as if they are the device's owner. This flaw can allow hackers to take over typical device function like sending messages and taking photos because users think malicious activity is a mobile app they use regularly.	
Source	https://gbhackers.com/strandhogg/amp/
Infected Industry	Smart Phones
Recommendation	Be careful before downloading Third party app

For any queries/recommendations:

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