CryptoGen Nepal

InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Critical PPP Daemon Flaw affects Linux Systems
2. Hackers compromised T-Mobile Employee to Steal User Data
3. Serious Nvidia Flaw Plagues Graphics Driver
4. Media Tek Bug Actively Exploited, affects Millions of Androids
5. Critical Zoho Zero-day Flaw Disclosed
6. Foodmandu Data Breach

03/09/2020

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. Critical PPP Daemon Flaw affects Linux Systems

Description

A Point-to-Point Protocol Daemon (PPPd) software comes installed on almost all the Linux based Operating Systems, as well as powers the firmware of many other networking devices is found vulnerable to remote code execution. The vulnerability is due to an error in validating the size of the input before copying the supplied data into memory. As the validation of the data size is incorrect, arbitrary data can be copied into memory and cause memory corruption which leads to execution of unwanted code. The vulnerability can be exploited by unauthenticated attackers to remotely execute arbitrary code on affected systems and take full control over them.

Source	https://thehackernews.com/2020/03/ppp-daemon-vulnerability.html
Infected Technology	Debian, Ubuntu, Fedora,SUSE Linux NetBSD, RedHat,,Cisco CallManager TP-Link Products
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2020-8597

2. Hackers Compromised T-Mobile Employee To Steal User Data

Description

T-Mobile has suffered a data breach incident that recently exposed personal and accounts information of both its employees and customers to unknown hackers. Hackers were able to compromise the email accounts of some of its employees that resulted in unauthorized access to the sensitive information contained in it, including details for its customers and other employees. The exposed data of an undisclosed number of affected users include their names, phone numbers, account numbers, rate plans and features, and billing information.

Source	https://thehackernews.com/2020/03/hackers-compromise-t-mobile-employees.html
Infected Technology	T-Mobile
Recommendation	Change Pin and Passcode Be aware of Phishing emails

3. Serious Nvidia Flaw Plagues Graphics Driver

Description

Nvidia's graphics processing unit (GPU) display driver is used in devices targeted for enthusiast gamers; it's the software component that enables the device's operating system and programs to use its high-level graphics hardware. The flaw exists in the control panel component of the graphics driver, which is a utility program helping users monitor and adjust the settings of their graphics adapter. An attacker with local system access can corrupt a system file in the control panel, which would lead to DoS or escalation of privileges or code-execution attacks.

Source	https://threatpost.com/gamer-alert-serious-nvidia-flaw-plagues-graphics-driver/153380/
Infected Industry	Nvidia
Recommendation	Update the latest patch released.
CVE_ID	CVE-2020-5957 CVE-2020-5958 CVE-2020-5959 CVE-2020-5960

4. Media Tek Bug Actively Exploited Affects Millions Of Android Devices

Description

The MediaTek bug meanwhile is an elevation-of-privilege flaw which is more specifically a root-access issue.This flaw is published by a developer which is easy to use and has already been used to build malicious apps that gain root access on Android devices. The critical bug can be exploited with a specially crafted file, also has an exploit already circulating in the wild which could enable remote code execution within the context of a privileged process.

Source	https://threatpost.com/mediatek-bug-actively-exploited-android/153408/
Infected Industry	Android devices
Recommendation	Update the latest patch released.
CVE_ID	CVE-2020-0069

5. Critical Zoho Zero-Day Flaw Disclosed

Description

A zero-day vulnerability has been found in the IT help desk Manage Engine software made by Zoho Corp. This serious vulnerability enables an unauthenticated, remote attacker to launch attacks on affected systems. The vulnerability exists in Zoho Manage Engine Desktop Central, an endpoint management tool to help users manage their servers, laptops, smart phones, and more from a central location. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Manage Engine Desktop Central. Authentication is not required to exploit this vulnerability.

Source	https://threatpost.com/critical-zoho-zero-day-flaw-disclosed/153484/
Infected Technology	Zoho
Recommendation	Update the latest patch released.
CVE_ID	CVE-2020-8794

6. Foodmandu Data Breach

Description

Nepal’s No. 1 online food delivery service provider company Foodmandu survived cyberattack on Saturday, 7th March and 50k user details were leaked. The cause of the breach is unknown but looking into @mr_mugger’s tweet, officials believe it was this user that leaked the sensitive info. The breached data contains names, phone numbers, email, address etc.

Source	https://myrepublica.nagariknetwork.com/news/foodmandu-s-website-hacked-50-thousand-users-data-dumped/
Infected Technology	Foodmandu
Recommendation	Change Password of Foodmandu Use MFA as possible

For any queries/recommendations:

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