December 12, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Researchers Detail New Attack Method to Bypass Popular Web Application Firewalls
- CVE-2022-1096: Google Chrome & Microsoft Edge (Chromium) V8 Type Confusion Vulnerability
- Critical Ping Vulnerability Allows Remote Attackers to Take Over FreeBSD Systems
- A new Linux flaw can be chained with other two bugs to gain full root privileges
- New BMC Supply Chain Vulnerabilities Affect Servers from Dozens of Manufacturers

CryptoGen Nepal

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.

Researchers Detail New Attack Method to Bypass Popular Web Application Firewalls

Description	
Web application firewalls (WAFs) from different manufacturers may be bypassed by a new attack technique, allowing hackers to infiltrate networks and possibly acquire confidential customer and company data. In order to filter, monitor, and block HTTP(S) traffic to and from a web application and defend against threats like cross-site scripting (XSS), file inclusion, and SQL injection, web application firewalls are a crucial line of protection. The attack is performed by appending JSON syntax to SQL Injection payload that a WAF is unable to decode and left the WAF blind to these attacks. By exploiting this effective methodology, attackers might get access to a backend database and utilize additional flaws and exploits to dump data directly to the server or through the cloud.	
Source	https://thehackernews.com/2022/12/researchers-detail-new-attack-method-to.html
Infected Technology	Web Application Firewalls (WAFs)
Recommendation	Adding parser that detects JSON syntax in SQL Injection and blocks it after spotting

CVE-2022-1096: Google Chrome & Microsoft Edge (Chromium) V8 Type Confusion Vulnerability

Description	
The Chromium Project developed the free and open-source V8 JavaScript engine for Chrome and other Chromium-based web browsers. The Google Chrome V8 Engine flaw, tracked as CVE-2022-4262, was called a "type confusion vulnerability" by CISA. A "type confusion vulnerability" in Google Chrome V8 could let a remote attacker use a malicious website with a specially created HTML page to potentially exploit heap corruption. Attackers can take advantage of this type of weakness by crashing the browser using a specially prepared HTML page. Type confusion issues can potentially be used by attackers to run arbitrary code.	
Source	https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/cve-2022-1096-google-chrome-microsoft-edge-chromium-v8-type-confusion-vulnerability https://www.darkreading.com/vulnerabilities-threats/google-chrome-flaw-added-to-cisa-patch-list
Infected Technology	Google Chrome
Recommendation	Update Google Chrome to the latest version to fix this vulnerability.
CVE_ID	CVE-2022-1096

SiriusXM Vulnerability Lets Hackers Remotely Unlock and Start Connected Cars

Description
Cybersecurity researchers have discovered a security flaw that exposes Honda, Nissan, Infiniti, and Acura vehicles to remote attacks via SiriusXM's connected vehicle service. The vulnerability may be exploited to unlock, start, locate, and horn any automobile in an unlawful way only by knowing the vehicle identifying number (VIN), according to researcher Sam Curry in a Twitter thread last week. More than 10 million cars in North America are believed to use SiriusXM's Connected Vehicles (CV) Services, including Acura, BMW, Honda, Hyundai, Infiniti, Jaguar, Land Rover, Lexus, Nissan, Subaru, and Toyota. The system is intended to provide a variety of safety, security, and convenience services, including automatic crash notification, enhanced roadside assistance, remote door unlock, remote engine start, stolen vehicle recovery assistance, turn-by-turn navigation, and integration with smart home devices, among others.The flaw is related to an authorization flaw in a telematics program, which allowed for the retrieval of a victim's personal information as well as the execution of commands on the vehicles by sending a specially crafted HTTP request containing the VIN number to a SiriusXM endpoint.

Source	https://thehackernews.com/2022/12/siriusxm-vulnerability-lets-hackers.html
Infected Technology	SiriusXM
Recommendation	Update to the latest version as the vulnerability has been patched by SiriusXM.

New Go-based Botnet Exploiting Dozens of IoT Vulnerabilities to Expand its Network

Description	
A unique Go-based botnet named Zerobot has been seen in the wild, expanding by taking advantage of roughly two dozen security flaws in Internet of Things (IoT) devices and other applications. The botnet "contains various modules, including self-replication, assaults on multiple protocols, and self-propagation," Fortinet FortiGuard Labs researcher Cara Lin stated. "It also connects with its command-and-control server via the WebSocket protocol." The attack, which is alleged to have begun after November 18, 2022, particularly singles out Windows and Linux operating systems to obtain control of susceptible machines. Zerobot takes its name from a propagation script that's used to collect the malicious payload after getting access to a host based on its microarchitecture implementation (e.g., "zero.arm64").The virus is designed to target a broad range of CPU architectures, such as i386, amd64, arm, arm64, mips, mips64, mips64le, mipsle, ppc64, ppc64le, riscv64, and s390x.	
Source	https://thehackernews.com/2022/12/new-go-based-zerobot-botnet-exploiting.html
Infected Technology	TOTOLINK routers, Zyxel firewalls, F5 BIG-IP, Hikvision and other IoT devices
Recommendation	It is recommended to use the most up-to-date versions of the systems and programs used and to prevent the shared IoC findings related to the botnet from the security solutions in use.

Critical Ping Vulnerability Allows Remote Attackers to Take Over FreeBSD Systems

Description	
A critical vulnerability in the ping module of the FreeBSD operating system, identified as CVE-2022-23093, was patched by the developers of the FreeBSD operating system. This vulnerability could have been used to execute code remotely. When using raw sockets, the ping utility must have elevated privileges. It can test whether a remote host is reachable using ICMP messages. When a setuid bit set is installed, it becomes accessible to non-privileged users. In other words, when ping executes, it creates the raw socket and then revokes its elevated privileges. It is advised that researchers update vulnerable systems to a supported FreeBSD stable or release / security branch (releng) dated after the correction date. The FreeBSD operating system's maintainers made it clear that there is no available workaround.	
Source	https://securityaffairs.co/wordpress/139300/hacking/cve-2022-23093-freebsd-systems-flaw.html
Infected Technology	Supported versions of FreeBSD and a stack-based buffer overflow
Recommendation	Upgrade vulnerable systems to a supported FreeBSD stable
CVE_ID	CVE-2022-23093

A new Linux flaw can be chained with other two bugs to gain full root privileges

Description
Researchers at the Qualys' Threat Research Unit demonstrated how to chain a new Linux vulnerability, tracked as CVE-2022-3328, with two other flaws to gain full root privileges on an affected system. The vulnerability resides in the snap-confine function on Linux operating systems, a SUID-root program installed by default on Ubuntu. The snap-confine is used internally by snap to construct the execution environment for snap applications, an internal tool for confining snappy applications. The CVE-2022-3328 is a Snapd race condition issue that can lead to local privilege escalation and arbitrary code execution. The Qualys Threat Research Unit (TRU) exploited this bug in Ubuntu Server by combining it with two vulnerabilities in multipathd called Leeloo Multipath (an authorization bypass and a symlink attack, CVE-2022-41974 and CVE-2022-41973), to obtain full root privileges.

Source	https://securityaffairs.co/wordpress/139209/hacking/three-linux-bugs-full-root-privileges.html#:~:text=The%20experts%20chained%20the%20CVE,of%20several%20distributions%2C%20including%20Ubuntu.
Infected Technology	Linux OS
Recommendation	Update to the latest version of the system as soon as patch releases.
CVE_ID	CVE-2022-41937 CVE-2022-41974

New BMC Supply Chain Vulnerabilities Affect Servers from Dozens of Manufacturers

Description	
The MegaRAC Baseboard Management Controller (BMC) software from American Megatrends (AMI) has three security issues that could allow remote code execution on susceptible servers. BMCs are privileged independent systems that are used in servers to administer the host operating system and low-level hardware settings, even while the machine is off. Due to these features, BMCs are a desirable target for threat actors looking to install persistent malware on machines that can withstand hard drive replacements and operating system reinstalls. The most serious of the problems is CVE-2022-40259 (CVSS score: 9.9), an instance of arbitrary code execution using the Redfish API that necessitates the attacker having at least minimal access to the target device. Furthermore, CVE-2022-40242 (CVSS score: 8.3) refers to a hash for a sysadmin user that can be stolen and exploited to acquire administrative shell access, while CVE-2022-2827 (CVSS score: 7.5) is a flaw in the password reset feature that may be used to find out whether an account with a particular username exists.	
Source	https://thehackernews.com/2022/12/new-bmc-supply-chain-vulnerabilities.html
Infected Technology	American Megatrends MegaRAC Baseboard Management Controller
Recommendation	Ensure that all remote server management interfaces and BMC subsystems in their environments are on their dedicated management networks and are not exposed externally and ensure internal BMC interface access is restricted to administrative users with ACLs or firewalls.
CVE_ID	CVE-2022-40259 CVE-2022-40242 CVE-2022-2827

Cisco warns of High-Severity unpatched flaw affecting IP Phones firmware

Description	
In a recent security advisory, Cisco warned of a high-severity weakness that might possibly allow a remote attacker to execute code or create a denial-of-service (DoS) scenario on IP Phone 7800 and 8800 Series firmware. The manufacturer of cisco routers said that it is developing a patch to fix the vulnerability, which is identified as CVE-2022-20968 (CVSS score: 8.1) and results from incomplete input validation of incoming Cisco Discovery Protocol (CDP) packets. By sending modified Cisco Discovery Protocol communication to a vulnerable device, an attacker might use this flaw. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device. Affected are Cisco IP phones with firmware versions 14.2 and earlier. There are no updates or solutions for the problem, according to the organization, thus a fix will be released in January 2023.	
Source	https://thehackernews.com/2022/12/cisco-warns-of-high-severity-unpatched.html
Infected Technology	Cisco IP Phone
Recommendation	Update the patch as soon as it is provided by Cisco.

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**

OUR SERVICES

Our services as information security company includes:


INFORMATION SECURITY AUDIT


VULNERABILITY ASSESSMENT


PENETRATION TESTING


MANAGED/CO.MANAGED SOC


INCIDENT RESPONSE


THREAT ANALYSIS


SERVER HARDENING


CYBER SECURITY CONSULTANT


INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/