December 19, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Samba Issues Security Updates to Patch Multiple High-Severity Vulnerabilities
- Researchers demonstrate how EDR, and Antivirus can be weaponized against users
- Hackers Actively Exploiting Citrix ADC and Gateway Zero-Day Vulnerability
- Zero-Day vulnerability discovered in Apple
- New GoTrim Botnet Attempting to Break into WordPress Sites' Admin Accounts

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.

Hackers Actively Exploiting Citrix ADC and Gateway Zero-Day Vulnerability	
Description	
Citrix Application Delivery Controller (ADC) and Gateway's zero-day vulnerability has been extensively exploited by APT5, according to the NSA. The significant remote code execution flaw, also known as CVE-2022-27518, might allow an unauthorized attacker to remotely control susceptible devices and execute commands. However, for the Citrix ADC or Citrix Gateway appliance to be setup as a SAML service provider (SP) or a SAML identity provider, it must be SAML compliant (IdP). Citrix reported that the weakness had been used in a "limited number of targeted attacks in the field."	
Source	https://thehackernews.com/2022/12/hackers-actively-exploiting-citrix-adc.html
Infected Technology	Citrix
Recommendation	Update to the latest version to fix this vulnerability.
CVE_ID	CVE-2022-27518

Zero-Day vulnerability discovered in Apple	
Description	
Apple on Tuesday rolled out security updates to iOS, iPadOS, macOS, tvOS, and Safari web browser to address a new zero-day vulnerability that could result in the execution of malicious code. Tracked as CVE-2022-42856, the issue has been described by the tech giant as a type of confusion issue in the WebKit browser engine that could be triggered when processing specially crafted content, leading to arbitrary code execution. It's worth noting that every third-party web browser that's available for iOS and iPadOS, including Google Chrome, Mozilla Firefox, and Microsoft Edge, and others, is required to use the WebKit rendering engine due to restrictions imposed by Apple.	
Source	https://thehackernews.com/2022/12/new-actively-exploited-zero-day.html
Infected Technology	Apple operating systems (iOS, macOS, iPadOS, tvOS)
Recommendation	Update to the latest version of the system.
CVE_ID	CVE-2022-42856

Samba Issues Security Updates to Patch Multiple High-Severity Vulnerabilities

Description
Samba has published software updates to address a number of vulnerabilities that, if exploited properly, might allow an attacker to take control of compromised systems.CVE-2022-38023, CVE-2022-37966, CVE-2022-37967, and CVE-2022-45141 have been fixed in versions 4.17.4, 4.16.8, and 4.15.13, which were published on December 15, 2022.Samba is an open source Windows interoperability package that provides file server, printer, and Active Directory services for Linux, Unix, and macOS operating systems. A brief description of each of the weaknesses is below - CVE-2022-38023 (CVSS score: 8.1) - Use of weak RC4-HMAC Kerberos encryption type in the NetLogon Secure Channel. CVE-2022-37966 (CVSS score: 8.1) - An elevation of privilege vulnerability in Windows Kerberos RC4-HMAC. CVE-2022-37967 (CVSS score: 7.2) - An elevation of privilege vulnerability in Windows Kerberos. CVE-2022-45141 (CVSS score: 8.1) - Use of RC4-HMAC encryption when issuing Kerberos tickets in Samba Active Directory domain controller (AD DC) using Heimdal. Microsoft originally released CVE-2022-37966 and CVE-2022-37967, which allow an adversary to get administrator rights, as part of its November 2022 Patch Tuesday upgrades. Microsoft first disclosed CVE-2022-37966 and CVE-2022-37967, which allow an adversary to get administrator rights, as part of its November 2022 Patch Tuesday upgrades. An unauthenticated attacker might use cryptographic protocol flaws in RFC 4757 (Kerberos encryption type RC4-HMAC-MD5) and MS-PAC (Privilege Attribute Certificate Data Structure standard) to circumvent security measures in a Windows AD system.

Source	https://thehackernews.com/2022/12/samba-issues-security-updates-to-patch.html
Infected Technology	Samba
Recommendation	Install the latest patches as soon as possible.

Researchers demonstrate how EDR, and Antivirus can be weaponized against users

Description
Different endpoint detection and response (EDR) and antivirus (AV) systems contain high severity security flaws that have been publicly revealed. These flaws might be used to create the devices data wipers. This wiper may delete basically any file on a system, including system files, and turn a machine fully unbootable while executing with the permissions of an unprivileged user. It does all of this without putting any code into the target files, making it completely undetected. By design, EDR software may continuously scan a computer for files that could be destructive or suspicious and take the required action, such quarantining or destroying them. In a word, the plan is to use specially constructed routes to mislead weak security software into wiping valid files and folders on the system and breaking the computer. This is accomplished by using a junction point, also known as a soft link, in which one directory on the computer acts as an alias for another directory. To put it another way, the attacker uses a junction to direct the program toward a different route, such as the C: drive, between the time the EDR software recognizes a file as dangerous and tries to remove the file from the system.

Source	https://thehackernews.com/2022/12/researchers-demonstrate-how-edr-and.html
Infected Technology	End Point Detection and Response Software
Recommendation	Update the EDR as soon as the patch is released.
CVE_ID	CVE-2022-37971, CVE-2022-45797, CVE-2022-4173

Fortinet Warns of Active Exploitation of New SSL-VPN Pre-auth RCE Vulnerability

Description
Fortinet published emergency patches on Monday for a critical security vulnerability in its FortiOS SSL-VPN product, which it claims is being actively abused in the wild.The significant problem, identified as CVE-2022-42475 (CVSS score: 9.3), is a heap-based buffer overflow vulnerability that might allow an unauthenticated attacker to execute arbitrary code via carefully crafted requests.The company stated that it is "aware of an instance where this vulnerability was exploited in the wild," advising users to install the patches as soon as possible. The following products are impacted by the issue - FortiOS version 7.2.0 through 7.2.2, FortiOS version 7.0.0 through 7.0.8, FortiOS version 6.4.0 through 6.4.10, FortiOS version 6.2.0 through 6.2.11, FortiOS 6K7K version 7.0.0 through 7.0.7, FortiOS-6K7K version 6.4.0 through 6.4.9, FortiOS-6K7K version 6.2.0 through 6.2.11, FortiOS-6K7K version 6.0.0 through 6.0.14. The American network security firm also revealed indicators of compromise (IoCs) connected with the exploitation attempts, such as IP addresses and artifacts found in the file system following a successful assault.The advice comes two months after Fortinet warned of another serious authentication bypass problem in FortiOS, FortiProxy, and FortiSwitchManager being actively weaponized (CVE-2022-40684, CVSS score: 9.6).

Source	https://thehackernews.com/2022/12/fortinet-warns-of-active-exploitation.html
Infected Technology	FortiOS SSL-VPN
Recommendation	Install the latest patches as soon as possible.

New GoTrim Botnet Attempting to Break into WordPress Sites' Admin Accounts

Description
A new Go-based botnet has been spotted scanning and brute-forcing self-hosted websites using the WordPress content management system (CMS) to seize control of targeted systems. This new brute forcer is part of a new campaign we have named GoTrim because it was written in Go and uses ':::trim:::' to split data communicated to and from the C2 server. it utilizes a bot network to perform distributed brute-force attacks to login to the targeted web server. A successful break-in is followed by the operator installing a downloader PHP script in the newly compromised host that, in turn, is designed to deploy the "bot client" from a hard-coded URL, effectively adding the machine to the growing network. In its present form, GoTrim does not have self-propagation capabilities of its own, nor can it distribute other malware or maintain persistence in the infected system. The primary purpose of the malware is to receive further commands from an actor-controlled server that include conducting brute-force attacks against WordPress and OpenCart using a set of provided credentials.

Source	https://thehackernews.com/2022/12/new-gotrim-botnet-attempting-to-break.html
Infected Technology	WordPress Sites
Recommendation	It is recommended that every website Admin should ensure that user accounts use a strong password.

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/