December 26, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Critical security flaws reported in Passwordstate Enterprise password manager
- Vice Society Ransomware Attackers Adopt Robust Encryption Methods
- Zerobot Botnet emerges as a growing threat with new exploits and capabilites
- Two New Security Flaws reported in Ghost CMS blogging software
- W4SP Stealer Discovered in Multiple PyPI Packages Under Various Names

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.

Critical security flaws reported in Passwordstate Enterprise password manager

Description

Multiple vulnerabilities have been discovered in the password management software Passwordstate that could allow an unauthenticated hacker to access users' plaintext passwords or gain greater privileges within the application. The vulnerabilities were reported by Swiss cybersecurity firm modzero AG and could potentially be used by an attacker to exfiltrate passwords from the system, overwrite stored passwords within the database, or even gain shell access to the host system. Passwordstate, which is developed by Australian company Click Studios and has over 29,000 customers, is widely used by IT professionals. One of the vulnerabilities also affects the Chrome browser extension for Passwordstate. A newer version of the extension, released on September 7, 2022, is available to address this issue. Multiple vulnerabilities in password management software Passwordstate could allow an attacker with a valid username to access users' plaintext passwords, overwrite passwords within the database, or achieve remote code execution. It is important for users to ensure they are using the latest version of the software and to follow good password security practices. Passwordstate suffered a supply chain attack in April 2021 that allowed hackers to install a backdoor on customers' machines. It is important to use secure software and protect against these types of attacks.

Source	https://thehackernews.com/2022/12/critical-security-flaw-reported-in.html
Infected Technology	Passwordstate Enterprise password manager
Recommendation	To protect against vulnerabilities and threats, users of Passwordstate's password management software should update to version 9.6 or later.
CVE_ID	• CVE-2022-3875 • CVE-2022-3876 • CVE-2022-3877

Vice Society Ransomware Attackers Adopt Robust Encryption Methods

Description

In their recent attacks targeting a variety of industries, the Vice Society ransomware actors have switched to yet another custom ransomware payload. "This ransomware variant, dubbed 'PolyVice,' employs a strong encryption scheme based on the NTRUEncrypt and ChaCha20-Poly1305 algorithms. Unlike other ransomware gangs, the cybercrime actor does not use in-house developed file-encrypting malware. Instead, it is known to use third-party lockers in their attacks, such as Hello Kitty, Zeppelin, and RedAlert ransomware.it has also been observed that the threat actor used call back phishing to trick victim into installing remote desktop software for initial access

Source	https://thehackernews.com/2022/12/vice-society-ransomware-attackers-adopt.html
Infected Technology	Windows Operating System
Recommendation	Employee must be aware of phishing emails and email security must be implemented.

Two New Security Flaws reported in Ghost CMS blogging software

Description

Researchers have discovered two security vulnerabilities in the open-source blogging platform Ghost. One of the vulnerabilities, known as CVE-2022-41654, is an authentication bypass issue that allows unprivileged users to make unauthorized changes to newsletter settings. The other vulnerability, known as CVE-2022-41697, is an enumeration issue in the login functionality that could lead to the disclosure of sensitive information. Ghost has released updates to address these vulnerabilities, but users running certain versions of the platform are required to update their software to protect against these flaws. Ghost is used on over 52,600 websites, primarily in the US, UK, Germany, China, France, Canada, and India.

Source	https://thehackernews.com/2022/12/two-new-security-flaws-reported-in.html
Infected Technology	JavaScript-based blogging platform.
Recommendation	Update to version 4.48.8 for versions 4.46.0 to 4.48.7, and update to version 5.22.7 for any version of v5 up to and including 5.22.6.
CVE_ID	• CVE-2022-41654 • CVE-2022-41697

Ransomware Hackers Using New Way to Bypass MS Exchange ProxyNotShell Mitigations

Description

Threat actors associated with the Play ransomware strain are using a never-before-seen exploit chain to overcome blocking policies for ProxyNotShell weaknesses in Microsoft Exchange Server in order to gain remote code execution (RCE) via Outlook Web Access (OWA). "The new exploit approach circumvents URL rewriting mitigations for the Autodiscover endpoint," CrowdStrike researchers Brian Pitchford, Erik Iker, and Nicolas Zilio said in a technical report published on Tuesday.Play ransomware, which initially appeared in June 2022, was found to use many of the same strategies as other ransomware families like as Hive and Nokoyawa, the latter of which was updated to Rust in September 2022. Investigations of various Play ransomware incursions by the cybersecurity firm revealed that initial access to the target environments was gained through the OWA endpoint rather than directly abusing CVE-2022-41040.The approach, dubbed OWASSRF, most likely exploits another serious hole recorded as CVE-2022-41080 (CVSS score: 8.8) to obtain privilege escalation, followed by exploiting CVE-2022-41082 for remote code execution. According to CrowdStrike, the adversary was able to drop legitimate Plink and AnyDesk executables to retain permanent access, as well as take efforts to cleanse Windows Event Logs on compromised servers to mask the malicious activity.Microsoft patched all three vulnerabilities as part of their Patch Tuesday upgrades for November 2022.It's uncertain whether CVE-2022-41080, like CVE-2022-41040 and CVE-2022-41082, was actively exploited as a zero-day.

Source	https://thehackernews.com/2022/12/ransomware-hackers-using-new-way-to.html
Infected Technology	Microsoft Exchange Server
Recommendation	Install the latest patches as soon as possible.

Zerobot Botnet emerges as a growing threat with new exploits and capabilites

Description	
The Zerobot DDoS botnet has received updates that allow it to target more internet-connected devices and expand its network. The malware, called DEV-1061 by Microsoft Threat Intelligence Center (MSTIC), spreads through vulnerabilities in web applications and IoT devices such as firewalls, routers, and cameras. The latest version of Zerobot also includes the ability to exploit vulnerabilities in Apache and Apache Spark, and new DDoS attack capabilities. The Zerobot DDoS botnet, also known as ZeroStresser, is being offered as a DDoS-for-hire service to other criminal actors and is being advertised for sale on various social media networks. Microsoft has found that the latest version of Zerobot targets unpatched and improperly secured devices, and also attempts to brute-force over SSH and Telnet on ports 23 and 2323 to spread to other hosts. Zerobot was among the 48 domains seized by the U.S. Federal Bureau of Investigation (FBI) this month for offering DDoS attack services to paying customers. The Zerobot DDoS botnet, also known as ZeroStresser, is a malware-as-a-service offered to other criminal actors that self-propagates to more susceptible systems and spreads by compromising devices with known vulnerabilities. Zerobot 1.1 includes seven new DDoS attack methods using protocols such as UDP, ICMP, and TCP, and is being sold on social media networks. Zerobot was among the domains seized by the U.S. Federal Bureau of Investigation (FBI) for offering DDoS attack services to paying customers.	
Source	https://thehackernews.com/2022/12/zerobot-botnet-emerges-as-growing.html
Infected Technology	Internet connected devices like firewalls, routers, and cameras.
Recommendation	Keep all software and devices up to date with the latest patches and updates.
CVE_ID	• CVE-2021-42013 • CVE-2022-33891

W4SP Stealer Discovered in Multiple PyPI Packages Under Various Names

Description

Threat actors have published a new batch of malicious packages to the Python Package Index (PyPI) with the intention of delivering information-stealing malware to compromised developer machines. W4SP Stealer's primary function is to steal user data, such as credentials, cryptocurrency wallets, Discord tokens, and other relevant files. It was created and published by an actor known as BillyV3, BillyTheGoat, and billythegoat356. The 16 rogue modules are as follows: modulesecurity, informmodule, chazz, randomtime, proxygeneratorbil, easycordey, easycordeyy, tomproxies, sys-ej, py4sync, infosys, sysuptoer, nowsys, upamonkws, captchaboy, and proxybooster. Previous versions of the attack chains have also been observed fetching next-stage Python code directly from a public GitHub repository before dropping the credential stealer.The increase in new copycat variants coincides with the removal of the GitHub repository containing the original W4SP Stealer source code, indicating that cybercriminals not affiliated with the operation are also using the malware to attack PyPI users.

Source	https://thehackernews.com/2022/12/w4sp-stealer-discovered-in-multiple.html
Infected Technology	PyPl Packages
Recommendation	Update PyPI packages security patches as soon as it gets released.

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/