June 27, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Backedoored Python Libraries found stealing AWS Secret keys
- Russian Hackers Exploiting Microsoft Follina Vulnerability Against Ukraine
- Critical PHP Vulnerability Exposes QNAP NAS Devices to Remote Attacks
- Zimbra patched memcached injection flaw that imperiled user credentials

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.

Backedoored Python Libraries found stealing AWS Secret keys

Description

A number of malicious Python packages have been identified in the official third-party software repository. The malicious packages were designed to exfiltrate AWS credentials and environment variables to a publicly exposed endpoint. Sharma from Sona-type said “Some of these packages either contain code that reads and exfiltrates your serets or use one of the dependencies that will do the job”. The stolen credentials were stored in a txt file which was accessible to anyone on the web.

Source	https://blog.sonatype.com/python-packages-upload-your-aws-keys-env-vars-secrets-to-web
Infected Technology	• Loglib-modules • Pyg-modules • Pygrata, Pygrata-util • Hkg-sol-utils
Recommendation	• Avoid using infected packages

Russian Hackers Exploiting Microsoft Follina Vulnerability Against Ukraine

Description

A Computer Emergency Team of Ukraine (CERT-UA) has warn of a new set of spare-phishing attacks exploiting the “Follina” flaw in the windows operating system to deploy password-stealing malware. Follina with the CVSS score of 7.8 concerns a case of remote code execution affecting windows support diagnostic tool (MSDT). The main purpose of the malware is to siphon data, including passwords and saved cookies, from several popular browsers such as Google Chrome, Microsoft Edge, and Mozilla Firefox.

Source	https://thehackernews.com/2022/06/russian-hackers-exploiting-microsoft.html
Infected Technology	Microsoft MSDT
Recommendation	Update latest patch available.
CVE_ID	CVE-2022-30190

Critical PHP Vulnerability Exposes QNAP NAS Devices to Remote Attacks

Description	
A significant, three-year-old PHP vulnerability that might be exploited to obtain remote code execution is now being fixed by QNAP, a Taiwanese manufacturer of network-attached storage (NAS) devices. Attackers can obtain remote code execution if the vulnerability is exploited. After updating the firmware, QNAP has recommended users who can't find the ransom letter to input the DeadBolt decryption key they got to contact QNAP Support for help. researching in-depth a new wave of DeadBolt ransomware assaults that target QNAP NAS units using QTS 4.x-outdated software.	
Source	https://thehackernews.com/2022/06/critical-php-vulnerability-exposes-qnap.htm
Infected Technology	PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24, and 7.3.x below 7.3.11 with nginx config
Recommendation	Update to latest patch available.
CVE_ID	CVE-2019-11043

Zimbra patched memcached injection flaw that imperiled user credentials

Description

Security researchers have discovered a memcached injection vulnerability in Zimbra, a commercial webmail provider, which might allow attackers to obtain login credentials without user involvement. Attackers might inject arbitrary memcached instructions into a targeted instance and cause an overwrite of arbitrary cached entries because newline characters (/r,/n) were not escaped in untrusted user input. Memcached servers process incoming data line by line and store key/value pairs that may be created and retrieved via a straightforward text-based interface. However, once a mailbox is compromised, "attackers can potentially escalate their access to targeted organizations and gain access to various internal services and steal highly sensitive information," researchers warned. The severity of the vulnerability (CVE-2022-27924) is listed as "high" (CVSS 7.5) rather than "critical."

Source	https://portswigger.net/daily-swig/business-email-platform-zimbra-patches-memcached-injection-flaw-that-imperils-user-credentials
Infected Technology	Versions below to latest patch
Recommendation	Patched versions are 8.8.15 with patch level 31.1 and 9.0.0 with patch level 24.1
CVE_ID	CVE-2022-27924

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/