August 22, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Multiple cloud vendors impacted by PostgreSQl vulnerability that exposed enterprise databases
- Vulnerability in open-source identity management system Free IPA could lead to XXE attacks
- Apple Releases Security Updates to Patch Two New Zero Day Vulnerabilities
- ÆPIC and SQUIP Vulnerabilities Found in Intel and AMD Processors
- New Google Chrome Zero-Day Vulnerability Being Exploited in the Wild.

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.

Multiple cloud vendors impacted by PostgreSQL vulnerability that exposed enterprise databases

Description	
Wiz Researchers has discovered flaws in the well-liked "PostgreSQL-as-a-Service" solutions provided by several cloud suppliers. As a result of PostgreSQL's permission model's inability to grant a user just a limited number of superuser access, cloud service providers had to make modifications to their software to give normal users a limited amount of superuser powers. The update allowed the team to run arbitrary commands on vendor-managed compute instances of several PostgreSQL-as-a-Service products, giving them access to other users' data without their knowledge who were utilizing the impacted service.	
Source	https://portswigger.net/daily-swig/multiple-cloud-vendors-impacted-by-postgresql-vulnerability-that-exposed-enterprise-databases
Infected Technology	PostgreSQL
Recommendation	• create a table with dummy content and create a malicious index function • alter the table owner to cloudsqladmin, GCP's superuser role • analyze the table and switch user-context to the table's owner, cloudsqladmin • call the malicious index function with the cloudsqladmin permission

Vulnerability in open-source identity management system Free IPA could lead to XXE attacks	
Description	
FreeIPA is a free and open-source identity management system and is the upstream project of Red Hat Identity Management. A flaw, tracked as CVE-2022-2414, was found in the pki-core package, a security advisory from Red Hat warns. By submitting carefully crafted HTTP requests, a remote attacker may be able to possibly obtain the content of any file. With XXE, you may inject arbitrary entities into XML documents and carry out malicious operations like accessing local files or making HTTP requests to a network within a computer. In the latter case, unpatched apps inside a corporate network might result in remote code execution (RCE).	
Source	https://portswigger.net/daily-swig/vulnerability-in-open-source-identity-management-system-free-ipa-could-lead-to-xxe-attacks
Infected Technology	Red Hat Enterprise Linux 6-9 and Red Hat Certificate System 9 and 10
Recommendation	Red Hat in all versions apart from Linux 6.
CVE_ID	CVE-2022-2414

Apple Releases Security Updates to Patch Two New Zero-Day Vulnerabilities

Description
On Wednesday, Apple published security patches for the iOS, iPadOS, and macOS platforms to fix two zero-day flaws that threat actors have previously used to harm the company's products. A WebKit out-of-bounds bug that might allow arbitrary code to be executed by parsing carefully prepared web content. A kernel bug that allows for out-of-bounds access that might be leveraged by malicious software to run arbitrary code with root capabilities. It added that it has improved bounds checking to address both problems and that it is aware the flaws may have been actively exploited. Although it's probable that they were employed as part of highly targeted intrusions, the corporation made no more statements about these assaults or the identity of the threat actors that carried them out.

Source	https://thehackernews.com/2022/08/apple-releases-security-updates-to.html
Infected Technology	Apple (iOS, iPadOS, and macOS) platforms
Recommendation	Update to the latest version (IOS 15.6.1, iPadOS 15.6.1, and macOS Monterey 12.5.1)
CVE_ID	CVE-2022-32893, CVE-2022-32894

ÆPIC and SQUIP Vulnerabilities Found in Intel and AMD Processors	
Description	
A team of researchers has disclosed information on a fresh flaw in Intel CPUs that lets attackers steal encryption keys and other sensitive data from the processors. The vulnerability, known as "PIC Leak," is the first of its type to architecturally reveal private information in a way similar to a "uninitialized memory read in the CPU itself. Researchers from Amazon Web Services, the Graz University of Technology, the Sapienza University of Rome, and the CISPA Helmholtz Center for Information Security carried out the study. The memory-mapped registers of the local Advanced Programmable Interrupt Controller (APIC) on Intel CPUs based on the Sunny Cove microarchitecture were found to be improperly initialized during the scan of the I/O address space. As a result, reading these registers architecturally produces outdated information from the microarchitecture. These registers enable reading of any data transported between the L2 and the last-level cache.	
Source	https://thehackernews.com/2022/08/pic-and-squip-vulnerabilities-found-in.html
Infected Technology	Intel CPUs
Recommendation	No security updates have been released
CVE_ID	CVE-2022-21233

Bumblebee loader used by hackers to attack Active Directory

Description	
Bumblebee is a malware loader that is used in post exploitation activities of active directory. The loader is associated with threat actors such as TrickBot, BazarLoader, and IcedID. Google's threat analysis group (TAG) discovered the loader in March of 2022 and is believed to propagate after initial access provided by spear phishing campaigns. The researchers said, "Distribution of the malware is done by phishing emails with an attachment or a link to a malicious archive containing Bumblebee," Cobalt strike adversary simulation framework along with AnyDesk remote desktop management software is deployed with bumblebee for lateral movement and persistence respectively. If a high privilege domain user is compromised, the attackers seize control of the Active Directory. According to the researchers, "Attacks involving Bumblebee must be treated as critical and this loader is known for ransomware delivery."	
Source	https://thehackernews.com/2022/08/hackers-using-bumblebee-loader-to.html
Infected Technology	Windows active directory
Recommendation	Install email security tools and frameworks to prevent phishing attacks.

New Google Chrome Zero-Day Vulnerability Being Exploited in the Wild.

Description	
Google released updates for the Chrome desktop browser on Tuesday to fix a high-severity zero-day vulnerability that is now being aggressively exploited. Insufficient intents validation of untrusted input has been identified as the problem. The tech giant has held off on disclosing more information about the flaw until most users have been informed. In a brief statement, Google said, "Google is aware that an attack for CVE-2022-2856 exists in the wild.	
Source	https://thehackernews.com/2022/08/new-google-chrome-zero-day.html
Infected Technology	Google Desktop for Windows, Linux, and Mac.
Recommendation	Update to version 104.0.5112.101 for macOS and Linux and 104.0.5112.102/101 for Windows.
CVE_ID	CVE-2022-2856

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/