May 2, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- New Privilege Escalation vulnerability name "Nimbuspwn"in Linux Operating System.
- Synology warns of critical Netatalk bugs in multiple products
- Cisco Patches 11 High-Severity Vulnerabilities in Security Products
- IBM Database Address Critical Vulnerabilities in Third-party XML Parser.
- Critical Vulnerabilities in Azure PostgreSQL Exposed User Databases

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.

New Privilege Escalation vulnerability name “Nimbuspwn”in Linux Operating System.

Description	
Microsoft has uncovered a number of vulnerabilities, collectively known as Nimbuspwn, that could allow an attacker to get root access to various Linux desktop endpoints. The flaws can be chained together to achieve root privileges on Linux systems, allowing attackers to install payloads such as a root backdoor and carry out other malicious acts via arbitrary root code execution. Furthermore, the flaws identified as CVE-2022-29799 and CVE-2022-29800 could be used to gain root access and deploy more complex threats like ransomware.	
Source	https://thehackernews.com/2022/04/microsoft-discovers-new-privilege.html
Infected Technology	Linux Endpoints
Recommendation	Update to the latest version of the Operating system as soon as possible.
CVE_ID	CVE-2022-29799 CVE-2022-29800

Synology warns of critical Netatalk bugs in multiple products

Description	
Network-attached storage (NAS) appliances of Synology are exposed to attacks by exploiting multiple critical Netatalk vulnerabilities. The vulnerabilities allow remote attackers to obtain sensitive information and possibly execute arbitrary code via a susceptible version of Synology DiskStation Manager and Synology Router Manager. The vulnerability was exploited (rated with a 9.8/10 severity score) to achieve remote code execution without authentication.	
Source	https://www.bleepingcomputer.com/news/security/synology-warns-of-critical-netatalk-bugs-in-multiple-products/
Infected Technology	Synology
Recommendation	Update to latest version
CVE_ID	CVE-2022-23121, CVE-2022-23122, CVE-2022-0194

Cisco Patches 11 High-Severity Vulnerabilities in Security Products

Description
There was a total of 19 vulnerabilities in Cisco's security solutions, 11 of which were rated as "high severity." The most serious of them is an FTD security flaw that arises due to improper handling of TCP traffic and might be exploited remotely without authentication to generate a denial of service (DoS) issue. An attacker might take advantage of this flaw by delivering a specially crafted stream of TCP communication through a vulnerable device. An attacker might utilize a successful exploit to force the device to reload, resulting in a DoS scenario. An attacker might send a maliciously engineered file to a device running the vulnerable software. A successful exploit might allow the attacker to place malicious files on the device, which they could subsequently access to carry out additional attacks, such as running arbitrary code with root capabilities on the device.

Source	https://www.securityweek.com/cisco-patches-11-high-severity-vulnerabilities-security-products
Infected Technology	Cisco Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), and Firepower Management Center (FMC)
Recommendation	Update new patches and the latest version.
CVE_ID	CVE-2022-20746

Critical Vulnerabilities in Azure PostgreSQL Exposed User Databases

Description	
ExtraReplica is the term given to the security weaknesses identified by Wiz researchers. The issues affected a database replication capability, hence the name. They influenced Azure Database for PostgreSQL Flexible Server, a fully managed PostgreSQL database-as-a-service. A malicious user might use an improperly anchored regular expression to overcome authentication and obtain access to other customers' databases by exploiting an elevated rights problem in the Flexible Server authentication procedure for a replication user.	
Source	https://thecybersecurity.news/general-cyber-security-news/microsoft-azure-vulnerability-exposes-postgresql-databases-to-other-customers-18581/
Infected Technology	Microsoft Azure
Recommendation	It is recommended that customer to enable private network access when setting up their Flexible Server instances.

IBM Database Address Critical Vulnerabilities in Third-party XML Parser.

Description	
To protect users from a pair of critical vulnerabilities in older versions of Expat, a third-party library, IBM has updated its data management platform Db2.Because to integer overflow concerns, both bugs received a CVSS score of 9.8 and might potentially allow attackers to execute arbitrary code on susceptible computers. Expat's XML GetBuffer (CVE-2022-23852) and doProlog methods include integer overflows (CVE-2022-23990). According to similar cautions from NetApp, which is working on solutions for some of its own vulnerable products, the issues "may lead to disclosure of sensitive information, addition or change of data, or Denial of Service (DoS)" if abused.	
Source	https://portswigger.net/daily-swig/ibm-database-updates-address-critical-vulnerabilities-in-third-party-xml-parser
Infected Technology	Db2 versions 9.7.x, 10.1.x, 10.5.x, and 11.1.x
Recommendation	Update to latest version (V9.7 FP11, V10.1 FP6, V10.5 FP11, and V11.1.4 FP6)
CVE_ID	CVE-2022-23852, CVE-2022-23990

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