March 28, 2022

INFOSEC WEEKLY

#MADE4SECURITY

Western Digital My Cloud OS update fixes critical vulnerability

OpenSSL Addresses High Severity DoS Issue

Honda bug lets a hacker unlock and start car via replay attack

SOPHOS fixes SQL injection vulnerability in UTM appliance.

VMware Issues Patches for Critical Flaws Affecting Carbon Black App Control

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.

Western Digital My Cloud OS update fixes critical vulnerability

Description	
The vulnerability that allows remote attackers to execute arbitrary code on the target device, without requiring authentication. The flaw was exploited by the NCC Group's EDG team members and relied on the open-source service named "Netatalk Service" which was included in MY Cloud OS. The patches of these vulnerability is released and update to the latest version is recommended.	
Source	https://www.bleepingcomputer.com/news/security/western-digital-my-cloud-os-update-fixes-critical-vulnerability/
Infected Technology	My Cloud OS
Recommendation	Update to latest version
CVE_ID	CVE-2022-23121

OpenSSL Addresses High Severity DoS Issue

Description	
The software flaw exposes cryptographic subsystems to the risk of rogue certifications. According to an OpenSSL security advisory, "the BN mod sqrt() function, which computes a modular square root, includes a problem that might lead it to loop forever for non-prime moduli. The infinite loop can be initiated by creating a certificate with invalid, explicit curve parameters. Any operation which requires the public key from the certificate will trigger the infinite loop. Attackers can use a self-signed certificate to trigger the loop during verification.	
Source	https://portswigger.net/daily-swig/openssl-drops-update-addressing-high-severity-denial-of-service-issue-in-ubiquitous-encryption-library
Infected Technology	OpenSSL versions 1.0.2, 1.1.1, and 3.0.
Recommendation	Update to latest OpenSSL versions 1.0.2zd,1.1.1n, 3.0.2

Honda bug lets a hacker unlock and start car via replay attack

Description

Multiple researchers revealed a vulnerability this week that may be used by a nearby attacker to remotely unlock and start various Honda and Acura car models. The vulnerability is a Man-in-the-Middle (MitM) attack, or more specifically, a replay attack, in which an attacker intercepts the RF signals normally sent from a remote key fob to the automobile, manipulates them, and re-sends them later to unlock the car at will.

Source	https://www.bleepingcomputer.com/news/security/honda-bug-lets-a-hacker-unlock-and-start-your-car-via-replay-attack/
Infected Technology	Man-in-the-Middle (MitM) attack or more specifically a replay attack on RF Signals of Honda Cars
Recommendation	Reset key fob from car dealership and rolling codes for authentication request
CVE_ID	CVE-2022-27254

SOPHOS fixes SQL injection vulnerability in UTM appliance.

Description

Sophos has patched a critical vulnerability in its all-in-one Universal Threat Management (UTM) appliances' software. A post-authentication SQL injection vulnerability in the Mail Manager component of the appliance created a means for attackers to run hostile code on a Sophos UTM appliance. The vulnerability was discovered by Sophos during internal security testing, can be resolved by updating to version 9.710 of the software, released earlier this month.

Source	https://portswigger.net/daily-swig/sophos-fixes-sql-injection-vulnerability-in-utm-appliance
Infected Technology	SOPHOS UTM
Recommendation	Update to the latest version 9.71
CVE_ID	CVE-2022-0386

VMware Issues Patches for Critical Flaws Affecting Carbon Black App Control	
Description	
VMware has addressed two significant security flaws in its Carbon Black App Control platform that may be exploited by a malicious actor to conduct malicious program on certain Windows installations. The attacker must already be logged in as an administrator or a highly privileged user to successfully exploit the vulnerabilities. VMware Carbon Black App Control is an application allow listing solution for locking down servers and important systems, preventing unauthorized modifications, and ensuring regulatory compliance. CVE-2022-22951 is a command injection vulnerability that potentially grant network access to the VMware App Control to an authorized, high-privileged actor. An attacker with administrator access to the VMware App Control might use CVE-2022-22952 to exploit a file upload vulnerability.	
Source	https://thehackernews.com/2022/03/vmware-issues-patches-for-critical.html
Infected Technology	VMware Carbon Black App Control
Recommendation	Update to latest version
CVE_ID	CVE-2022-22951, CVE-2022-2295

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