May 30, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Cisco Issues Patch for New IOS XR Zero-Day Vulnerability
- Critical 'Pantsdown' BMC Vulnerability Affects QCT Servers Used in Data Centers
- Zyxel warns of flaws impacting firewalls, Aps, and controllers
- Zoom Flaws Could Let Attackers Hack Victims Just by Sending them a Message
- VMware Authentication Bypass Vulnerability Has Been Patched

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.

Cisco Issues Patch for New IOS XR Zero-Day Vulnerability

Description

An unauthenticated, remote attacker can get access to the Redis instance operating within the NOSi container by exploiting this vulnerability. These flaws are caused by IGMP packets being handled incorrectly. An attacker could take advantage of these flaws by delivering specially designed IGMP traffic to a vulnerable device. An attacker could use a successful exploit to crash the IGMP process or cause memory exhaustion, causing other processes to become unstable. Interior and external routing protocols are examples of these procedures, but they are not restricted to them.

Source	https://thehackernews.com/2022/05/cisco-issues-patches-for-new-ios-xr.html
Infected Technology	This vulnerability affects Cisco 8000 Series Routers that are running Cisco IOS XR Software version 7.3.3 and have the health check RPM installed
Recommendation	Effectively disable the health check from the device. Then remove the health check RPM from the device.
CVE_ID	CVE-2022-20821

Critical 'Pantsdown' BMC Vulnerability Affects QCT Servers Used in Data Centers

Description	
The critical "Pantsdown" Baseboard Management Controller (BMC) bug has been discovered in Quanta Cloud Technology (QCT) servers. An attacker executing code on a vulnerable QCT server may 'hop' from the server host to the BMC and extend their attacks to the server management network, where they could theoretically continue and get rights to other BMCs on the network, and so gain access to other servers. A successful attack of the vulnerability might give a threat actor complete control of the server, allowing them to rewrite the BMC firmware with malicious code, install persistent malware, exfiltrate data, and even brick it.	
Source	https://thehackernews.com/2022/05/critical-pantsdown-bmc-vulnerability.html
Infected Technology	OCT server models (D52BQ-2U, D52BQ-2U 3UPI, D52BV-2U) with BMC version 4.55.00
Recommendation	Update to the latest version.
CVE_ID	CVE-2019-6260

Zyxel warns of flaws impacting firewalls, Aps, and controllers

Description	
A security advisory was published by Zyxel to warn admins about multiple vulnerabilities affecting a wide range of firewall. AP, and AP controller products. Since the vulnerabilities were not rated as critical but but still significant on their own and can be abused by threat actors as part of exploit chains.	
Source	https://www.bleepingcomputer.com/news/security/zyxel-warns-of-flaws-impacting-firewalls-aps-and-controllers/
Infected Technology	USG/ZyWALL, USG FLEX, ATP, VPN, NSG firewalls, NXC2500 and NXC5500, AP controllers, and a range of Access Point products, including models of the NAP, NWA, WAC, and WAX series
Recommendation	Upgrade the device as soon as possible.
CVE_ID	CVE-2022-0734, CVE-2022-26531, CVE-2022-26532, CVE-2022-0910

VMware Authentication Bypass Vulnerability Has Been Patched

Description	
A proof-of-concept exploit code for a critical authentication bypass vulnerability in numerous VMware products, which allows attackers to get admin rights and access. While Shodan only identifies a small number of VMware appliances vulnerable to attacks aimed at this flaw, certain healthcare, education, and state government entities are at a higher risk of being targeted.	
Source	https://www.bleepingcomputer.com/news/security/researchers-to-release-exploit-for-new-vmware-auth-bypass-patch-now /
Infected Technology	VMware Workspace ONE Access, Identity Manager, and vRealize Automation.
Recommendation	• Update and install the latest version or patch of the software.
CVE_ID	CVE-2022-22972

Zoom Flaws Could Let Attackers Hack Victims Just by Sending them a Message

Description	
A security flaw in zoom chat can be used to infect another user via chat by sending specially designed Extensible Messaging and Presence Protocol (XMPP) messages and running malicious malware. Because Zoom's chat functionality is based on the XMPP protocol, successful exploitation of the flaws could allow an attacker to force a vulnerable client to impersonate a Zoom user, connect to a malicious server, and even download a rogue update, resulting in arbitrary code execution via a downgrade attack.	
Source	https://thehackernews.com/2022/05/new-zoom-flaws-could-let-attackers-hack.html
Infected Technology	It affects in Zoom application software
Recommendation	• Update to the latest version (5.10.0)
CVE_ID	CVE-2022-22784, CVE-2022-22785, CVE-2022-22786, CVE-2022-22787

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/