January 24, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Google Details Two Zero-Day Bugs Reported in Zoom Clients and MMR Servers
- Cisco Issues Patch for Critical RCE Vulnerability in RCM for StarOS Software
- Researchers Hack Olympic Games App
- McAfee Agent bug lets hackers run code with Windows SYSTEM privileges
- Red Cross Hit via Third-Party Cyberattack
- Microsoft fixes Patch Tuesday bug that broke VPN in Windows 10 and 11

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.

Google Details Two Zero-Day Bugs Reported in Zoom Clients and MMR Servers

Description	
Google Project Zero security researcher Natalie Silvanovich discovered a zero-click attack surface for zoom and Multimedia Routers (MMR) Servers that transmit audio and video content between clients in on-premise deployments, which could have been exploited to crash the service, execute malicious code and even leak arbitrary areas of its memory. Silvanovich discovered that by sending a malicious chat message, it is possible to modify the contents of a buffer that allows reading various data types, leading the client and MMR server to crash.	
Source	https://thehackernews.com/2022/01/google-details-two-zero-day-bugs.html
Infected Technology	Zoom and MMR Servers.
Recommendation	Stay updated with latest security patches.
CVE_ID	CVE-2021-34423

Cisco Issues Patch for Critical RCE Vulnerability in RCM for StarOS Software

Description	
Cisco Systems has released patches to address a severe security flaw in Redundancy Configuration Manager (RCM) for Cisco StarOS Software, which may be exploited by an unauthenticated, remote attacker to execute arbitrary code and take control of vulnerable systems. An attacker might take advantage of this flaw by connecting to the device and going to the service while in debug mode "Cisco said in a statement. "If the exploit is effective, the attacker will be able to run arbitrary commands as the root user.	
Source	https://thehackernews.com/2022/01/cisco-issues-patch-for-critical-rce.html
Infected Technology	Redundancy Configuration Manager (RCM) of Cisco StartOS Software
Recommendation	• Install the official security patch immediately.
CVE_ID	CVE-2022-20649

Researchers Hack Olympic Games App

Description	
The MY2022 app, meant for use by participants of this year's Winter Olympic Games in Beijing, has a "devastating fault," which was discovered by Canadian cybersecurity researchers. The MY2022 app has critically flawed encryption, putting users' private data and any other data exchanged via it at risk of being stolen. This also implies that data might be read by the Chinese through Wi-Fi hotspots at hotels, airports, and Olympic venues.	
Source	https://www.infosecurity-magazine.com/news/researchers-hack-olympic-games-app/
Infected Technology	MY2022 App
Recommendation	Update the App to its latest version available till date.

McAfee Agent bug lets hackers run code with Windows SYSTEM privileges

Description	
McAfee Agent a client-side component of McAfee ePolicy Orchestrator was discovered to have a security vulnerability that allowed Windows enabling attackers to escalate privileges and execute arbitrary code with SYSTEM privileges. With the release of McAfee Agent 5.7.5, high severity local privilege escalation (LPE) problems tagged as CVE-2022-0166 were corrected and offered security upgrades. All versions prior to 5.7.5 are vulnerable, allowing unprivileged attackers to execute code with the NT AUTHORITY SYSTEM account privileges.	
Source	https://www.bleepingcomputer.com/news/security/mcafee-agent-bug-lets-hackers-run-code-with-windows-system-privileges/
Infected Technology	McAfee Agent.
Recommendation	Update McAfee Agent with the latest security patches attached with the release of McAfee Agent 5.7.5.
CVE_ID	CVE-2022-0166

Red Cross Hit via Third-Party Cyberattack	
Description	
The International Committee of the Red Cross (ICRC) acknowledged a cyberattack against its data servers that compromised personal and confidential information of more than 515,000 "extremely vulnerable people." The attack targeted an external company in Switzerland with whom the ICRC has a contract to hold its data. Officials have shut down the systems, hampering their ability to run certain programs. The ICRC's main concern is the risk of confidential information being released, which might harm the people Red Cross and Red Crescent are trying to protect.	
Source	https://www.darkreading.com/attacks-breaches/red-cross-hit-via-third-party-cyberattack
Infected Technology	Personal data and confidential information of more than 515,000 "highly vulnerable people," of Red Cross.
Recommendation	Shutdown the systems until workarounds are identified to continue work without risk. Take precautions until the risk has been maintained and solved.

Microsoft fixes Patch Tuesday bug that broke VPN in Windows 10 and 11

Description	
Microsoft's January upgrades, issued last week, created a slew of issues, by damaging VPN connections in Windows 10, Windows 11, and Windows Server versions 2022, 20H2, 2019, and 2016 affected "IPSEC connections that contain a Vendor ID," as well as L2TP and IPSEC IKE VPN connections. The built-in VPN client in Windows as well as third-party VPN clients that use these types of connections are mostly affected. Patch Tuesday's current set of upgrades caused issues with Windows Server, including unexpected domain controller reboots and Hyper-V virtual machine startup failures. Microsoft has provided The fixes for the issues have been provided by Microsoft as of today.	
Source	https://www.theverge.com/2022/1/18/22889670/microsoft-windows-server-update-vpn-refs-domain-patch
Infected Technology	IPSEC, L2TP, and IPSEC IKE VPN connections in Windows 10, Windows 11, and Windows Server versions 2022, 20H2, 2019, and 2016.
Recommendation	Apply the fixes provided by Microsoft to resolve the issues.

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