July 26, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Overly permissive ACL in Windows allows Local privilege escalation
- Linux kernel flaw allows unprivileged user to gain root access
- Oracle Warns of Critical Remotely Exploitable WebLogic Server Flaws
- New PetitPotam attack allows takeover of Windows domains
- OpenManage Enterprise vulnerabilities patched by Dell
- MacOS malware steals Telegram accounts, Google Chrome data

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.

Overly permissive ACL in Windows allows Local privilege escalation

Description	
Microsoft's Windows 10 and upcoming Windows 11 are vulnerable to local privilege escalation that allows low-lever user to gain access to System files, when exploited can be used to execute arbitrary code with high privilege. The flaw is due to the access provided to some registry files that allow privilege escalation. The vulnerability has been acknowledged by Microsoft while the patch is still pending.	
Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934
Infected Technology	Windows 10 build 1809 and later
Recommendation	Apply the workaround listed in OEM's advisory Update the patch, once released by OEM
CVE-ID	CVE-2021-36934

Linux kernel flaw allows unprivileged user to gain root access

Description	
Researchers from Qualys has identified a string conversion vulnerability in Linux Kernel's seq_file allows a local unprivileged attacker to create mount and delete deep directory structure which allows the local user to gain root level access in the system. The vulnerability is assumed to have infected various distribution of Linux and has been verified in Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04, Debian 11, and Fedora 34 Workstation.	
Source	https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909
Infected Technology	Linux Kernel
Recommendation	Update the patch released by your Linux Distributor for the CVE
CVE-ID	CVE-2021-33909

Oracle Warns of Critical Remotely Exploitable WebLogic Server Flaws

Description	
Oracle's quarterly Critical Patch Update included 342 fixes across numerous products, some of which might be used by a remote attacker to seize control of a system. CVE-2019-2729 is a serious deserialization vulnerability in Oracle WebLogic Server Web Services via XMLDecoder that can be remotely exploited without authentication.	
Source	https://www.oracle.com/security-alerts/cpuapr2021.html
Infected Technology	Oracle Weblogic versions 11.1.2.4 and 11.2.5.0
Recommendation	Update the latest available patch.
CVE-ID	• CVE-2021-2394 • CVE-2021-2397 • CVE-2021-2382 • CVE-2021-2378 • CVE-2021-2376 • CVE-2021-2403

New PetitPotam attack allows takeover of Windows domains

Description	
PetitPotam is a new NTLM relay attack that allows threat actors to gain control of a domain controller, and hence an entire Windows domain. Microsoft Active Directory Certificate Services, a public key infrastructure (PKI) server that may be used to authenticate users, services, and computers on a Windows domain, is utilized by many companies. To cause a domain controller to authenticate against a rogue NTLM relay, which would then send the request through HTTP to the domain's Active Directory Certificate Services. A Kerberos ticket granting ticket (TGT) would be provided to the attacker, allowing them to assume the identity of any device on the network, even a domain controller.	
Source	https://twitter.com/remiescourrou/status/1418232548677804032
Infected Technology	Windows AD
Recommendation	Update the latest available patch.

OpenManage Enterprise vulnerabilities patched by Dell

Description	
The first critical vulnerability patched by Dell was an improper authentication vulnerability that could allow a remote attacker to "hijack an elevated session or perform unauthorized actions by sending malformed data." An attacker does not need any authentication to exploit this vulnerability. Another critical bug patched was an OS command injection bug in RACADM and IPMI tools that could allow a remote, authenticated malicious user that already has high privileges to execute arbitrary OS commands.	
Source	https://www.dell.com/support/kbdoc/en-vn/000189680/openmanage-enterprise-versions-3-4-through-3-6-1-contain-known-security-vulnerability-cve-2021-21596-as-described-in-dsa-2021-113
Infected Technology	Dell OpenManage Enterprise
Recommendation	Update your Dell OpenManage Enterprise
CVE-ID	• CVE-2021-21546 • CVE-2021-21585 • CVE-2021-21596

MacOS malware steals Telegram accounts, Google Chrome data

Description	
A new malware named XCSSET has been discovered by security researchers to steal login information from multiple apps, enabling its operators to steal accounts. XCSSET has been seen to collect sensitive information from infected computers and send them to Command and Control (C2) server. Researchers at Trend Micro explain that copying the stolen folder on another machine with Telegram installed gives the attackers access to the victim's account.Researchers have also noted that the XCSSET is evolving and adapting continuously and has been seen to leverage a zero-day vulnerability on macOS version.	
Source	https://www.trendmicro.com/en_us/research/20/h/xcsset-mac-malware--infects-xcode-projects--uses-0-days.html
Infected Technology	macOS applications (Telegram, Chrome)
Recommendation	keep your macOS enabled devices and its applications up to date

Universal Decryptor for REvil ransomware

Description	
After a widespread supply chain ransomware attack on software vendor Kaseya, the officials confirms they recieved a universal decryptor to decrypt their impacted data. More than 1500 networks was said to be infiltrated on this incident. A sum of 60 MSP (Managed Service Providers) was said to be impacted as they were using Kaseya's VSA remote management product which was impacted by the REvil ransomware.	
Source	https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-23rd-2021
Infected Technology	Kaseya VSA Remote Management
Recommendation	Use patch released by Kaseya for their products
CVE-ID	N/A

Apple fixes bug that breaks iPhone WiFi when joining rogue hotspots

Description	
Apple has released security upgrades to fix dozens of vulnerabilities in iOS and macOS, including a serious iOS flaw known as WiFiDemon that may result in a denial of service or arbitrary code execution. It might be able to break an iPhone's Wi-Fi functionality by connecting to hotspots with SSIDs containing the " percent " character if the attack was successful (i.e., percent p percent s percent s percent s percent s percent When the bug is activated on a vulnerable iPhone, iPad, or iPod, it prevents it from making Wi-Fi connections, even after rebooting or renaming the Wi-Fi hotspot.	
Source	https://twitter.com/vm_call/status/1405937492642123782
Infected Technology	iOS
Recommendation	Update the latest available patch released by OEM
CVE-ID	CVE-2021-30800

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/