November 29, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- ProxyLogon flaw used by attackers to hijack Email Threads
- Microsoft releases patch for a zero-day vulnerability
- VMware Warns of Newly Discovered Vulnerabilities in vSphere Web Client
- Hackers Exploiting New Windows Installer Zero-day
- A new linux malware spotted scheduled for February 31st

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.

ProxyLogon flaw used by attackers to hijack Email Threads

Description	
A Microsoft Exchange Server vulnerability named ProxyLogon allowed attackers to bypass authentication and impersonate as an admin. Even though Microsoft has released one click patch, there are still numerous Exchange Server vulnerable to this attack and attackers are leveraging this to hijack email chains by malspamming replies to ongoing threads.	
Source	https://blog.talosintelligence.com/2021/10/squirrelwaffle-emerges.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29
Infected Technology	Microsoft Exchange Server
Recommendation	Apply Mitigation Tool released by Microsoft

Microsoft releases patch for a zero-day vulnerability

Description	
Microsoft has released a free unofficial patch to protect Windows users from a local privilege escalation zero-day vulnerability. The vulnerability is known to exist in the MDM or Mobile Device Management Service impacting windows 10. According to a security researcher, this issue, when exploited will allow to gain admin privileges. Though there are two specific conditions which requires attackers to exploit this vulnerability. Microsoft urges to update the security patch to address this issue.	
Source	https://blog.0patch.com/2021/11/micropatching-unpatched-local-privilege.html
Infected Technology	Windows 10 v1809 and later
Recommendation	Update the latest available patch.
CVE_ID	CVE-2021-34484

VMware Warns of Newly Discovered Vulnerabilities in vSphere Web Client

Description	
VMware has patched two security flaws in vCenter Server and cloud foundation that may be exploited by a remote attacker to obtain access to sensitive data. A hostile actor with network access to vCenter Server's port 443 may exploit the problem to obtain access to sensitive information. The most serious vulnerability is an arbitrary file read vulnerability in the vSphere Web Client. The vSphere Web Client (FLEX/Flash) includes an SSRF (Server Side Request Forgery) vulnerability in the vSAN Web Client (vSAN UI) plug-in, which may be exploited by reading a URL request outside of vCenter Server or an internal service.	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0027.html
Recommendation	Update the latest available patch.
CVE_ID	CVE-2021-21980, CVE-2021-22049

Hackers Exploiting New Windows Installer Zero-day

Description	
Attackers are exploiting new variant of a recently disclosed privilege escalation vulnerability to potentially execute arbitrary code on fully-patched systems. According to Cisco Talos, they detected malware samples in the wild that are attempting to take advantage of this vulnerability	
Source	https://blog.talosintelligence.com/2021/11/attackers-exploiting-zero-day.html
Infected Technology	Microsoft Windows
Recommendation	Apply patches release by Microsoft
CVE_ID	CVE-2021-41379

A new linux malware spotted scheduled for February 31st

Description	
Researcher have identified a new RAT, dubbed CronRAT, for that is scheduled to run on February 31st. The malware uses cron job to schedule execution in February 31st. CronRAT injects payment skimmers such as Magecart in service-side code to prevent browser based solutions. The multi-layer stealth capacity of the malware from getting detected from various security solutions.	
Source	https://sansec.io/research/cronrat
Infected Technology	Linux
Recommendation	• Update the knowledge base of Security products regularly • Review running processes and implement endpoint protection

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/