November 8, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Hackers Exploiting GitLab Unauthenticated RCE Flaw in the wild
- Critical vulnerability in Linux Kernel's TIPC Module
- 'Pink' botnet malware infected over 1.6 million devices
- Phisher impersonating cybersecurity firm to harvest e-mail credentials
- Microsoft makes web content filtering generally available

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.

Hackers Exploiting GitLab Unauthenticated RCE Flaw in the wild

Description	
A fixed significant remote code execution vulnerability in Gitlab's web interface has been discovered to be being exploited in the field, making many GitLab systems vulnerable to assaults. Because of the vulnerability's unauthenticated nature, exploitation activity is predicted to escalate, making it critical.	
Source	https://security.humanativaspa.it/gitlab-ce-cve-2021-22205-in-the-wild/
Infected Technology	Gi
Recommendation	Update the latest available patch

Critical vulnerability in Linux Kernel's TIPC Module

Description	
Cybersecurity researchers from SentinelLabs has disclosed a security flaw in Linux Kernel's Transparent Inter Process Communication (TIPC) module that can be exploited locally and remotely to execute arbitrary code. The flaw is a heap overflow vulnerability with the severity of 9.8. The vulnerability can be exploited over network and locally to gain kernel privileges that could lead to compromise of full system.	
Source	https://www.sentinelone.com/labs/tipc-remote-linux-kernel-heap-overflow-allows-arbitrary-code-execution/
Infected Technology	Linux Kernel 5.10-rc1 to 5.15
Recommendation	Ensure that their Linux kernel version is not between 5.10-rc1 to 5.15.
CVE_ID	CVE-2021-43267

‘Pink’ botnet malware infected over 1.6 million devices

Description	
Researchers from Qihoo 360’s Netlab security team has identified possibly the largest botnet attack observed in the wild in last six year. The botnet has infected over 1.6 million devices which are majorly located in China. The main goal of the mass infection is to launch DDoS attack and inserting advertisement in HTTP websites. The botnet uses third party services such as GitHub, peer-to-peer (P2P) network and central C2C server for communication vial encrypted channel.	
Source	https://blog.netlab.360.com/pink-en/
Recommendation	Network admins can identify the malicious traffic using the IoCs provided in the source link to.

Phisher impersonating cybersecurity firm to harvest e-mail credentials

Description	
A campaign has been discovered by researchers at Armorblox where phishers are impersonating Proofpoint to harvest Microsoft Office 365 and Google email credentials. The email seemed like Proofpoint sent a link and when victim clicked a link, they were redirected to a splash page that spoofed Proofpoint branding and contained login links for different email providers. The attack included dedicated login page spoofs for Microsoft and Google.	
Source	https://www.armorblox.com/blog/proofpoint-credential-phishing/
Infected Technology	Cloud Based Services
Recommendation	Cyber security awareness and strong password hygiene

"Trojan Source" conceals vulnerabilities in Source Code

Description	
Threat actors could be allowed to inject visually deceptive malware through a novel class of vulnerabilities. The deception passes as permissible. However, the logic defined by the source code is altered that may introduce numerous first-party and supply chain risks. Identified as "Trojan Source attacks", the technique exploits text-encoding standards in a way that makes the output different from that intended. Also, the vulnerabilities cannot be perceived directly as the characters are deemed permissible.	
Source	https://thehackernews.com/2021/11/new-trojan-source-technique-lets.html
Infected Technology	C, C++, C#, JavaScript, Java, Rust, Go, Python
Recommendation	Make proper use of a Software supply chain
CVE-ID	CVE-2021-42574 CVE-2021-42694

Remote Root Access through SSH Key in Cisco Policy suite

Description	
Cisco has released security updates addressing a vulnerability that allows perpetrators to login as root user in multiple Cisco products. Threat actors could exploit the vulnerability by connecting to any affected device through SSH.	
Source	https://cybersecuritynews.com/hard-coded-key-based-ssh-authentication-flaw/
Infected Technology	• Catalyst PON Switch CGP-ONT-1P • Catalyst PON Switch CGP-ONT-4P • Catalyst PON Switch CGP-ONT-4PV • Catalyst PON Switch CGP-ONT-4PVC • Catalyst PON Switch CGP-ONT-4TVCW
Recommendation	Update to Cisco Policy Suite Releases 21.2.0 or later
CVE-2021-40444	CVE-2021-40119

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/