March 21, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- OpenSSL cert parsing bug causes infinite denial of service loop
- Node.js security: Parse Server RCE vulnerability
- TrickBot Malware Abusing MikroTik routers as proxies for CNC.
- B1txor20 botnet exploits Log4j flaw by using DNS tunnels.

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.

OpenSSL cert parsing bug causes infinite denial of service loop

Description	
A security update was released to address a vulnerability that affects OpenSSL library. This vulnerability could activate an infinite loop function and leads to denial of service of service conditions and could cause significant business interruption, long-term financial repercussions, and brand reputation degradation. This vulnerability impacts a few deployment scenarios such as TLS clients consuming server certificates, TLS servers consuming client certificates, hosting providers taking certificates or private keys from customers, certificate authorities parsing certification requests from subscribers and anything else which parse ASN.1 elliptic curve parameters.	
Source	https://www.bleepingcomputer.com/news/security/openssl-cert-parsing-bug-causes-infinite-denial-of-service-loop/
Infected Technology	OpenSSL version 1.0.2 to 1.0.2zc, 1.1.1 to 1.1.1n, and 3.0 to 3.0.1
Recommendation	Update to latest version.
CVE_ID	CVE-2022-0778

Node.js security: Parse Server RCE vulnerability

Description	
The popular API server Module for Node/Express, Parse Server were urged to apply the fix for RCE vulnerability. The RCE vulnerability was discovered in default configuration with MongoDB which has been confirmed in Ubuntu and Windows version of the software. The root cause of the security problem was prototype pollution.	
Source	https://portswigger.net/daily-swig/node-js-security-parse-server-remote-code-execution-vulnerability-resolved
Infected Technology	Node.js (below v.4.10.7)
Recommendation	Users are advised to upgrade to at least v.4.10.7 of Parse Server. The most recent build available is 5.0.0, which also bundles new and improved file upload security controls.
CVE_ID	CVE-2022-24760

TrickBot Malware Abusing MikroTik routers as proxies for CNC.

Description	
On Wednesday, Microsoft revealed that the TrickBot malware employs a previously unknown technique that involves utilizing compromised Internet of Things (IoT) devices as a go-between for communicating with command-and-control (C2) servers. TrickBot, which first appeared in 2016 as a banking trojan, has grown into a sophisticated and persistent threat, thanks to its modular architecture, which allows it to adapt its tactics to suit different networks, environments, and devices, as well as provide access-as-a-service for next-stage payloads like the Conti ransomware.	
Source	https://thehackernews.com/2022/03/trickbot-malware-abusing-hacked-iot.html
Infected Technology	MikroTik Routers
Recommendation	Continuous monitoring of the logs and connection going in and off of the routers.
CVE_ID	CVE-2018-14847

B1txor20 botnet exploits Log4j flaw by using DNS tunnels.

Description	
Qihoo 360's Netlab security team discovered a backdoor that targets Linux systems and adds them to a botnet for the purpose of downloading and installing rootkits. The researchers dubbed the malware B1txor20 and was first observed propagating through the Log4J vulnerability. B1txor20 utilizes DNS tunneling to establish communication channels with C2 servers. The malware is capable of stealing sensitive information and command execution while obfuscating itself to remain hidden002E	
Source	https://thehackernews.com/2022/03/new-b1txor20-linux-botnet-uses-dns.html
Infected Technology	Linux platform
Recommendation	It is advised to secure end points of a network using security measures such as IDS, IPS, Firewalls and anti-viruses.

New Vulnerability in CRI-O Engine Lets Attackers Escape Kubernetes Containers	
Description	
An attacker might use cr8escape, a recently reported security flaw in the Kubernetes container engine CRI-O, to break out of containers and get root access to the host. "An attacker can use CVE-2022-0811 to perform a range of operations on goals, including malware execution, data exfiltration, and lateral movement across pods," CrowdStrike researchers John Walker and Manoj Ahuje wrote in a report released this week. CRI-O is a lightweight alternative to Docker that pulls container images from registries and launches an Open Container Initiative (OCI)-compatible runtime like runC to spawn and run container processes.	
Source	https://www.crowdstrike.com/blog/cr8escape-new-vulnerability-discovered-in-cri-o-container-engine-cve-2022-0811/
Infected Technology	Kubernetes containers
Recommendation	Upgrade to 1.18 and higher version of cri-o
CVE_ID	CVE-2022-0811

DirtyMoe Botnet Gains New Exploits in Wormable Module to spread Rapidly

Description	
DirtyMoe malware has obtained new worm-like propagation capabilities, allowing it to spread its reach without any human engagement. Many victims are at danger because many computers still use unpatched systems or weak passwords; one worm module can create and attack hundreds of thousands of private and public IP addresses each day; many victims are at risk because many machines still use unpatched systems or weak passwords. The DirtyMoe botnet has been active since 2016, and it uses external exploit kits like PurpleFox or implanted Telegram Messenger installers to carry out cryptojacking and distributed denial-of-service (DDoS) assaults. The main purpose of the worming module is to gain RCE and install a new DirtyMoe instance with administrator capabilities.	
Source	https://thehackernews.com/2022/03/dirtymoe-botnet-gains-new-exploits-in.html
Infected Technology	PurpleFox or Telegram Messenger, PHP, Java Deserialization, and Oracle Weblogic Servers
Recommendation	Update to latest version.
CVE_ID	CVE-2019-9082, CVE-2019-2725, CVE-2019-1458, CVE-2017-0144, MS15-076

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

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/