August 9, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft Exchange servers scanned for ProxyShell vulnerability
- Actively exploited bug bypasses authentication on millions of routers
- 0-day RCE in Cisco Adaptive Security Device Manager
- NET library for Go and Rust affected by Ip address validation vulnerability
- "Prometheus", a malware-as-a-service (MaaS) solution
- BlackMatter ransomware targets VMware ESXi servers

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.

Microsoft Exchange servers scanned for ProxyShell vulnerability

Description	
ProxyShell is the term given to three vulnerabilities that, when chained together, allow unauthenticated, remote code execution on Microsoft Exchange servers. After specialized details were released at the Black Hat event, threat actors are now aggressively looking for the Microsoft Exchange ProxyShell remote control code implementation flaw.	
Source	https://twitter.com/GossiTheDog/status/1423991791326482443
Infected Technology	Microsoft Exchange Server
Recommendation	Update the latest available patch
CVE-ID	CVE-2021-34473, CVE-2021-34523, CVE-2021-31207

Actively exploited bug bypasses authentication on millions of routers

Description	
Threat actors actively attack a serious authentication bypass vulnerability affecting Arcadyan firmware-based home routers in order to take them over and distribute Mirai botnet malicious payloads. The flaw is a severe path traversal flaw in the web interfaces of routers running Arcadyan firmware that might allow unauthenticated remote attackers to circumvent authentication.	
Source	https://blogs.juniper.net/en-us/security/freshly-disclosed-vulnerability-cve-2021-20090-exploited-in-the-wild
Infected Technology	Many well-known Vendors
Recommendation	Update the latest available patch
CVE-ID	CVE-2021-20090

0-day RCE in Cisco Adaptive Security Device Manager

Description	
Cisco has released a security advisory revealing the Remote code execution bug in Cisco Adaptive Security Device Manager Launcher. The vulnerability exists due to a lack of signature verification between ADSM and Launcher for specific code. An attacker can exploit the vulnerability by launching man-in-the-middle attack between Launcher and ADSM allowing injection of arbitrary code. The exploit allows execution of arbitrary code in victim's OS with privilege provided to ADSM Launcher. The vulnerability has not been patched and no workaround has been provided by OEM until now.	
Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW
Infected Technology	Cisco ADSM 7.16(1.150) and earlier
Recommendation	Update the patch once released by OEM
CVE-ID	CVE-2021-1585

NET library for Go and Rust affected by IP address validation vulnerability

Description	
Commonly used net library in Go and Rust language is found to be vulnerable to mixed-format IP address validation. The library fails to handle mixed-format IP address in scenarios where decimal IPv4 address contains preceding 0 allowing attacker to launch attack as SSRF and RFI. The vulnerability was demonstrated in DEFCON and a fix has already been submitted to library's git.	
Source	https://sick.codes/sick-2021-015 https://sick.codes/sick-2021-016
Infected Technology	Net library for Rust and Go
Recommendation	Use updated library
CVE-ID	CVE-2021-29922, CVE-2021-29923

"Prometheus", a malware-as-a-service (MaaS) solution

Description	
Various cybercriminal groups are making use of "Prometheus", a malware-as-a-service solution to propagate and deploy payloads as Campo Loader, Hancitor, IcedID, QBot, Buer Loader, and SocGholish. The said MaaS solution, which is a Traffic Direction System (TDS), is available for purchase on underground platforms for $250 a month. Articles and documentations to enable and configure Prometheus can be found easily everywhere. Prometheus redirects visitors to phishing and malicious sites when users click on a link to a Google Doc, a HTML file that redirects the user to a compromised site on which Prometheus. Backdoor is installed, or a link to a web shell through their emails and collects information as IP address, User-Agent, Referrer header, time zone, and language data) and then forwards this data to the Prometheus admin panel. The Admin panel follows by forwarding a command to redirect users to a particular URL or send a malicious Word or Excel document and then redirecting them to a legitimate site immediately after downloading the file, to make it seem like the file was downloaded from a safe source.	
Source	https://thehackernews.com/2021/08/a-wide-range-of-cyber-attacks.html
Recommendation	Be cautious about all communications receive and do not open any attachments contained in a suspicious email.

BlackMatter ransomware targets VMware ESXi servers

Description	
VMware ESXi is one of the most popular virtual machine platforms, there are ransomware operations which has started to target virtual machines. BlackMatter is believed to be a rebrand of DarkSide varient as researchers found similar routines. Targeting ESXi servers have been found to be very efficient as it allows attackers to encrypt multiple servers at once.	
Source	https://www.bleepingcomputer.com/news/security/linux-version-of-blackmatter-ransomware-targets-vmware-esxi-servers/
Infected Technology	ESXi Server
Recommendation	Apply patches for well-known vulnerabilities and monitor infrastructure for any indication of threats

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/