December 13, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- SonicWall Urges Customers to patch critical SMA Flaw Immediately
- Grafana Releases Security Patch After Severe Bug Exploit Goes Public
- Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird
- Malware called NginRAT targeting popular Nginx web server
- Botnet operators (Manga aka Dark Mirai) found targeting RCE Vulnerability in TP-Link Product

CryptoGen Nepal

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of sec security-related 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 the o offensive side of 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 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, Bug Crowd, under armor, 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.

SonicWall Urges Customers to patch critical SMA Flaw Immediately

Description	
SonicWall has urged customers to update the SMA 100 series appliances that they have been using to the latest version UpToDate. The discovery of multiple security vulnerabilities has been impacting SMA 200, 210, 400, 410, and 500v products which have been running versions 9.0.0.11-31 and earlier. Successful exploitation of the flaw can potentially cause denial-of-service (DoS) conditions. While there has been no evidence of the vulnerabilities being exploited, as SonicWall devices have become a lucrative target for threats to launch malicious actions, it has been highly recommended to quickly move to the updated version to apply patches.descriptionOne	
Source	https://thehackernews.com/2021/12/sonicwall-urges-customers-to.html?&web_view=true
Infected Technology	SonicWall SMA products
Recommendation	• Update SMA 100 series appliances
CVE_ID	CVE-2021-20038, CVE-2021-20039, CVE-2021-20040, CVE-2021-20041, CVE-2021-20042, CVE-2021-20043, CVE-2021-20044, CVE-2021-20045

Grafana Releases Security Patch After Severe Bug Exploit Goes Public

Description	
A new critical security weakness has been disclosed by Mozilla and provided fixes to address the vulnerability that could be potentially exploited by an adversary to crash a vulnerable application and even execute arbitrary code. The vulnerability resides update to the vulnerability. The vulnerability impacts the company's main Grafana dashboard used globally to monitor and aggregate logs from across their local and remote networks. All Grafana self-hosted servers that run 8. x versions are considered vulnerable. The issue was patched with the release of Grafana 8.3.1, 8.2.7, 8.1.8, and 8.0.7. in a cross-platform Network Security Service which is a collection of open-source cryptographic computer libraries designed to enable cross-platform development of client-server applications. After security researchers released proof-of-concept code to exploit the critical vulnerability described as a path traversal vulnerability whitlow an attacker to read files outside the application's folder, Grafana Labs has released an emergency security	
Source	https://therecord.media/grafana-releases-security-patch-after-exploit-for-severe-bug-goes-public/?web_view=true
Infected Technology	NSS versions prior to 3.73 or 3.68.1 ESRGrafana Dashboard
Recommendation	• Update the Grafana application for the newly released security update
CVE_ID	CVE-2021-43798

Mozilla Patches High-Severity Vulnerabilities in Firefox, Thunderbird

Description	
Mozilla released security updates for the Firefox browser and Thunderbird mail client to address various web attacks and vulnerabilities, including six that have a high severity rating. The successful exploitation of these vulnerabilities could result in full system compromise by executing a union of arbitrary code. The high severity vulnerabilities could result in the target URL being exposed and asynchronous functions being executed during navigation, and another vulnerability can result in heap buffer overflow because of incorrect type conversion of sizes from 64bit to 32bit integers. Mozilla also patched a potential spoofing attack and a use-after-free caused by Gc not tracing live pointers for macOS. The patches for these four high-severity vulnerabilities were shipped for Firefox, Firefox ESR, and Thunderbird Users.	
Source	https://www.securityweek.com/mozilla-patches-high-severity-vulnerabilities-firefox-thunderbird?&web_view=true
Infected Technology	Firefox Browser and Thunderbird Mail
Recommendation	• Update the Security Updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. • Encourage organizations to apply the available patches as soon as possible.
CVE_ID	CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539

Windows 10 Drive-By RCE Triggered by Default URI Handler

Description	
Researchers have discovered a drive-by remote code-execution bug in windows 10 via Internet Explorer 11//Edge Legacy (a default browser on windows 10 PCs). It can enable attackers to see or modify data via the user interface that they normally can't get at. The issue lies in the Windows 10/11 default Uniform Resource Identifier (URIs) handler for Office apps.	
Source	https://threatpost.com/windows-10-rce-uri-handler/176830/
Infected Technology	ms-officecmd: URIs, Windows 10
Recommendation	• Stay updated with the latest version of the windows product and its patch. • Beneficial Security advise against using Internet Explorer 11/Edge Legacy as it is no more supported by Microsoft and had 1.87 p.c share of the browser marketplace (as of Might 2020) and is no longer considered safe

Malware called NginRAT targeting popular Nginx web server

Description	
Researchers have discovered a new type of malware that hides inside the Nginx servers. NginRAT works as a server-side Magecart that injects itself into a Nginx process and is used to steal information from e-commerce servers. The malware makes changes to the core functionality of the Linux host system	
Source	https://cyware.com/news/nginrat-a-new-stealth-malware-exclusively-for-nginx-servers-0f951a5b
Infected Technology	e-commerce servers (North America and Europe)
Recommendation	• Use of LD_L1BRARY_PATH (with typo) may reveal the presence of this particular NginRAT version. • To find any active process, run the command: $ sudo grep -al LD_L1BRARY_PATH /proc/*/environ | grep -v self/ /proc/17199/environ /proc/25074/environ • Which will show any compromised processes and can be killed by: kill -9 <PID>

Botnet operators (MANGA aka Dark Mirai) found targeting RCE Vulnerability in TP-Link Product

Description	
The MANGA botnet operators have been discovered abusing a new vulnerability in the TP-Link TL-WR840N EU V5. The malicious script (tshit.sh) identifies infected machines architecture and downloads matching payloads before waiting for a command from the C2 server to carry out a denial-of-service (DoS) attack	
Source	https://cyware.com/news/manga-found-targeting-rce-vulnerability-in-tp-link-product-04e6f717
Infected Technology	TP-Link TL-WR840N EU V5
Recommendation	• Update the devices frequently. • Change the default credentials with stronger ones
CVE_ID	CVE-2021-41653

Mirai-based Botnet – Moobot Targets Hikvision Vulnerability

Description	
Last September 18th, A command injection vulnerability in the web server of some Hikvision product. Due to the insufficient input validation, attacker can exploit the vulnerability to launch a command injection attack by sending some messages with malicious commands.	
Source	https://www.fortinet.com/blog/threat-research/mirai-based-botnet-moobot-targets-hikvision-vulnerability?&web_view=true
Infected Technology	Hikvision Product (version 210628 and above)
Recommendation	Apply the official Patch released by HIKVISION.
CVE_ID	CVE-2021-3620

1.6 Million WordPress sites under cyber-attack from over 16.000 IP addresses

Description
As many as 1.6 million WordPress sites have been targeted by an active large-scale attack campaign originating from 16,000 IP addresses by exploiting weaknesses in four plugins and 15 Epsilon Framework themes.

Source	https://thehackernews.com/2021/12/16-million-wordpress-sites-under.html?&web_view=true
Infected Technology	Four plugins Kiwi Social Share (<= 2.0.10), WordPress Automatic (<= 3.53.2), Pinterest Automatic (<= 4.14.3), PublishPress Capabilities (<= 2.3) and 15 Epsilon Framework themes.
Recommendation	WordPress site owners running any of the aforementioned plugins or themes are recommended to apply the latest fixes.

Over 300,000 MikroTik Devices found vulnerable to remote hacking bugs

Description
At least 300,000 IP addresses associated with MikroTik devices have been found vulnerable to multiple remotely exploitable security vulnerabilities that have since been patched by the popular supplier of routes and wireless ISP devices.

Source	https://thehackernews.com/2021/12/over-300000-mikrotik-devices-found.html?&web_view=true
Infected Technology	MikroTik Devices
Recommendation	Lookout for software updates, use secure password, check devices firewall to restrict remote access to unfamiliar parties, and look for unusual scripts.
CVE_ID	CVE-2018-14847

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/