January 25, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Severe Flaws affect DNSMasq DNS Forwarder
- SonicWall Hacked Using -Day Bugs in Its Own VPN Product
- Signal, Facebook, Google chat apps bugs let attackers to spy on users
- Chrome 88 Drops Flash, Patches Critical Vulnerability
- Cisco fixes critical pre-auth bugs in SD-WAN, cloud license manager
- Attackers Steal E-mails, Info from OpenWrt Forum
- Hundreds of Networks Still Host Devices Infected with VPNFilter Malware
- Critical Vulnerabilities in 123contactform-for-wordpress WordPress Plugin

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.

1. Severe Flaws affect DNSMasq DNS Forwarder

Description

Multiple vulnerabilities have been uncovered in DNSMasq, an open-source software used for caching Domain Name System responses (DNS). A total of seven flaws, collectively called “DNSSpooq” by Israeli research firm JSOF highlights the weakness in the DNS architecture of DNSMasq making it powerless against attacks such as mounting DNS cache poisoning and remote execution of malicious code. DNSMasq was vulnerable to DNS cache poisoning attack allowing attacker to poison multiple domain names at ones under seconds of few minutes without the requirement of any special needs. In some cases, the DNSMasq was also configured to listen WAN interface hence, the attack was possible directly from the internet.

Source	https://www.jsof-tech.com/disclosures/dnspooq/
Infected Technology	DNSMasq software
CVE_ID	CVE-2020-25684, CVE-2020-25685, CVE-2020-25686
Recommendation	Update to the latest version (2.83 or above)

2. SonicWall Hacked Using -Day Bugs in Its Own VPN Product

Description

SonicWall, a popular internet security provider of firewall and VPN products, on late Friday disclosed that it fell victim to a coordinated attack on its internal systems. The San Jose-based company said the attacks leveraged zero-day vulnerabilities in SonicWall secure remote access products such as NetExtender VPN client version 10.x and Secure Mobile Access (SMA) that are used to provide users with remote access to internal resources. They identified a coordinated attack on its internal systems by highly sophisticated threat actors exploiting probable zero-day vulnerabilities on certain SonicWall secure remote access products.

Source	https://thehackernews.com/2021/01/exclusive-sonicwall-hacked-using-0-day.html
Infected Technology	• NetExtender VPN client version 10.x • Secure Mobile Access (SMA) version 10.x
Recommendation	Consider not using the infected technology until the vulnerability is patched.

3. Signal, Facebook, Google chat apps bugs let attackers to spy on users

Description

Logic bugs present in multiple video conferencing mobile applications such as Signal, Google Duo, Facebook Messenger, JioChat and Mocha messaging apps was identified by Natalie Silvanovich. Silvanovich, a Google Project Zero based security research found that these vulnerabilities allowed attackers to listen to user's surroundings without permission before the person on the other end picked up the call. The attackers could also transmit audios or videos to the affected device without the consent of the user by using a total of five vulnerabilities. Although the vulnerabilities have been patched, earlier the attacker was able to force targeted device to transmit audio without requiring the need of gaining code execution

Source	https://googleprojectzero.blogspot.com/2021/01/the-state-of-state-machines.html
Infected Technology	Signal, Google Duo, Facebook Messenger JioChat and Mocha messaging apps

4. Chrome 88 Drops Flash, Patches Critical Vulnerability

Description

Google has released Chrome 88 to the stable channel with several security improvements inside, including patches for 36 vulnerabilities, one of which is rated critical severity, and dropped support for Adobe Flash. The new browser iteration arrives with patches for a total of 36 vulnerabilities, 26 of which were reported by external researchers. The flaws can be exploited if the user visits or is redirected to a specially crafted webpage. The most important of these is CVE-2021-21117, an insufficient policy enforcement issue in Cryptohome that was rated critical severity. Exploitation of the bug could result in arbitrary code execution in the context of the browser.

Source	https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html
Infected Technology	Google Chrome
CVE-ID	CVE-2021-21117
Recommendation	Upgrade Google Chrome to its latest version.

5. Cisco fixes critical pre-auth bugs in SD-WAN, cloud license manager

Description

Cisco has released security updates to resolve pre-authentical remote code execution (RCE) vulnerabilities affecting Cisco Smart Software Manager software and multiple SD-WAN products. SD-WAN software works on the domain of managing wide-area networks (WAN). Smart Software Manager is a cloud-based management solution for Cisco licenses. The vulnerabilities allowed unauthenticated attackers to perform buffer overflow and command injection bugs for executing arbitrary code hence, running arbitrary command on underlying operating systems of devices running the vulnerable release of Cisco Smart Software Manager Satellite software and SD-WAN. Cisco has released a software to resolve the vulnerabilities in versions 6.3.0 and later and has renamed to software to Cisco Smart Software Manager On-Prem.

Source	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn
Infected Technology	SD-WAN products and Cisco Smart Software Manager Satellite releases 5.1.0 and earlier • SD-WAN vBond Orchestrator Software • SD-WAN vEdge Cloud Routers • SD-WAN vEdge Routers • SD-WAN vManage Software • SD-WAN vSmart Controller Software
CVE_ID	CVE-2021-1300, CVE-2021-1138, CVE-2021-1140 CVE-2021-1142
Recommendation	Consider applying security updates provided by cisco

6. Attackers Steal E-mails, Info from OpenWrt Forum

Description

The forum supporting the community for OpenWrt suffered a security breach over the weekend, giving hackers access to e-mail addresses, user handles and additional private forum user information. According to the security notice posted to the forum's home page, forum was breached in the early hours of Saturday Jan 16, though how attackers got in remains unknown. As the forum is often visited by those developing commercial routers, devices and software based on OpenWrt firmware, the thereat actors could use this information as a gateway into these companies. Commercial routers compatible with OpenWrt include devices from Netgear, Zyxel, TP-Link and Linksys.

Source	https://lists.openwrt.org/pipermail/openwrt-announce/2021-January/000008.html
Infected Technology	OpenWrt Forum
Recommendation	Consider resetting password for accessing OpenWrt Forum.

7. Hundreds of Networks Still Host Devices Infected with VPNFilter Malware

Description

According to the researchers at cybersecurity firm Trend Micro, the VPNFilter malware is still present in hundreds of networks and malicious actors could take control of the infected devices. VPNFilter Malware, identified in 2018 has been targeting large number of routers and network-attached storage (NAS) devices from ASUS, D-Link, Huawei, Linksys, MicroTik, Netgear, QNAP, TP-Link, Ubiquiti, UPVEL, and ZTE. It is believed to be operated by Russian threat actor Sofacy, with possible involvement from Sandworm, VPNFilter emerged as a major threat right from the start: 50 impacted device models, the potential to compromise critical infrastructure, and approximately 500,000 bots observed across 54 countries.

Source	https://www.trendmicro.com/en_ca/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html
Infected Technology	Routers and NAS devices from ASUS, D-Link, Huawei, Linksys, MicroTik, Netgear, QNAP, TP-Link, Ubiquiti, UPVEL, and ZTE.
Recommendation	Consider replacing infected routers and NAS.

8. Critical Vulnerabilities in 123contactform-for-wordpress WordPress Plugin

Description

A number of vulnerabilities were found in 123contactform-for-wordpress WordPress plugin. These critical vulnerabilities allow attackers to arbitrarily create posts and inject malicious files to the website without any form of authentication. With over 3k+ installations, the 123contactform-for-wordpress plugin was designed to help site owners add web forms, surveys, quizzes, or polls from a 123FormBuilder account to their WordPress website or blog. However, the plugin owners didn't provide a patch to fix these vulnerabilities. Instead, they took the plugin down from the WordPress Plugin Repository.

Source	https://blog.sucuri.net/2021/01/critical-vulnerabilities-in-123contactform-for-wordpress-wordpress-plugin.html?web_view=true
Infected Technology	Websites using 123contactform-for-wordpress WordPress Plugin version <= 1.5.6
Recommendation	Uninstall the plugin and find alternative solution.

9. New Reolink P2P Vulnerabilities Show IoT Security Camera Risks

Description

Nozomi Networks Labs has discovered vulnerabilities in the Peer-to-Peer (P2P) feature of a commonly used line of security cameras – Reolink. It was found that the communication between the NVR and the P2P Client occurred in clear text. The consequence of this design choice is that anybody who can access client/NVR traffic as it traverses the internet can access its audio/video payload—with no confidentiality for the parties involved. Furthermore, it was found that the NVR sends cleartext username and passwords to the Reolink Servers.

Source	https://us-cert.cisa.gov/ics/advisories/icsa-21-019-02
Infected Technology	Reolink devices that use P2P: • RLC-4XX series • RLC-5XX series • RLN-X10 series
Recommendation	Consider upgrading the firmware to its latest version.

10. Vulnerability in shazam application lead to expose location of Android and IOS Users

Description

A British IT security researcher Ashley King, discovered a vulnerability in popular Shazam application that allowed an attacker to steal the precise location of a user simply by clicking a link. This vulnerability affected more than 100 million users at the time having the potential to compromise the physical security of these users marking its severity. Talking about the vulnerability, how it worked was that an attacker could send a malicious link to their intended victim. If the victim opened it, this would automatically open the Shazam app and execute the malware resulting in the victim's location data being sent to the attacker.

Source	https://ash-king.co.uk/blog/Shazlocate-abusing-CVE-2019-8791-CVE-2019-8792
Infected Technology	Shazam, Android, IOS
CVE-ID	CVE-2019-8791, CVE-2019-8792
Recommendation	Consider not to open any forwarded links if you are not sure about it.

11. Fully-Functional Exploit Released Online for SAP Solution Manager Flaw

Description

Cybersecurity researchers have warned of a publicly available fully-functional exploit that could be used to target SAP enterprise software. The exploit leverages a vulnerability that stems from a missing authentication check in SAP Solution Manager (SolMan) version 7.2. A researcher from Onapsis said that a successful exploitation could allow a remote unauthenticated attacker to execute highly privileged administrative tasks in the connect ed SAP SMD Agents. The critical flaw resided in SolMan's User Experience Monitoring (formerly End-user Experience Monitoring or EEM) component, thus putting every business system connected to the Solution Manager at risk of a potential compromise.

Source	https://nvd.nist.gov/vuln/detail/CVE-2020-6207
Infected Technology	SAP Enterprise Software
CVE_ID	CVE-2020-6207

12. Attackers can exploit Windows RDP Servers to Amplify DDoS Attacks

Description

Researchers from Netscout discovered the Cybercriminals can exploit Microsoft Remote Desktop Protocol (RDP) as a powerful tool to amplify distributed denial-of-service (DDoS attacks) where attackers can abuse RDP to launch UDP reflection/amplification attacks with an amplification ratio of 85.9:1. However, not all RDP servers can be used in this way. It's possible only when the service is enabled on port UDP port 3389 running on standard TCP port 3389. Leveraging Windows RDP servers in this way has significant impact on victim organizations, including "partial or full interruption of mission-critical remote-access services," as well as other service disruptions due to transit capacity consumption and associated effects on network infrastructure.

Source	https://www.netscout.com/blog/asert/microsoft-remote-desktop-protocol-rdp-reflectionamplification
Infected Technology	Windows, RDP
Recommendation	Consider to deploy Windows RDP servers behind VPN concentrators to prevent them from being abused to amplify DDoS attacks.

13. Drupal releases fix for critical vulnerability with known exploits

Description	

Drupal has released a security update to address a critical vulnerability in a third-party library with documented or deployed exploits available in the wild. According to Drupal's security advisory, the vulnerability is caused by a bug in the PEAR Archive Tar library used by the CMS tracked as CVE-2020-36193. The bug causes out-of-path extraction vulnerabilities via "write operations with Directory Traversal due to inadequate checking of symbolic links." Successful exploitation requires access to user accounts with basic permissions on servers with uncommon module configurations. Exploiting the Drupal vulnerability is only possible if the CMS is configured to allow and process .tar, .tar.gz, .bz2, or .tlz file uploads. Following exploitation, attackers can modify or delete all data and can also gain access to all non-public data available on the compromised server.

Source	https://www.drupal.org/sa-core-2020-012
Infected Technology	Drupal
CVE-ID	CVE-2020-36193
Recommendation	• Drupal 9.1 users should update to 9.1.3 • Drupal 9.0 users should update to 9.0.11 • Drupal 8.9 users should update to 8.9.13 • Drupal 7 users should update to 7.78 • Consider disabling uploads of .tar, .tar.gz, .bz2, or .tlz files to temporarily mitigate the issue.

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**