June 07
2021

INFOSEC WEEKLY

#MADE4SECURITY

- Critical Bugs affect Realtek Wi-Fi Module
- Zero-Day exploit impacts a WordPress Plugin
- SonicWall Patches Command Injection Flaw in Firewall Management Application
- Siemens Patches Major PLC Flaw that Bypasses Its 'Sandbox' Protection
- Vulnerability in Lasso Library Impacts Products from Cisco, Akamai
- Cisco fixed High-Severity issues in Webex, SD-WAN, ASR 5000 software
- Apache Pulsar bug allowed account takeovers in certain configurations

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. Critical Bugs affect Realtek Wi-Fi Module

Description	
The Realtek Wi-Fi module has been identified as critically vulnerable. The module can be used by threat actors to gain elevated privileges and hijack wireless communication. The successful exploitation of this vulnerable module could allow the threat actors to gain complete control over the Wi-Fi module. The actors could also be able to gain root access to the OS embedded within the device that uses this Wi-Fi module. This flaw affects all the embedded and IoT devices that use this module for Wi-Fi connection. The attacker could also escalate this vulnerability by masquerading as a legitimate access point and send malicious encrypted traffic on the target devices, any device connected to the vulnerable Wi-Fi module could be the target for the attack.	
Source	https://www.vdoo.com/blog/realtek-wifi-vulnerabilities-zero-day
Infected Technology	Realtek RTL8195A Wi-Fi module
CVE ID	CVE-2020-27301, CVE-2020-27302
Recommendation	• Consider updating the firmware to its latest version. • Consider using a strong private WPA2 passphrase if the device's firmware cannot be updated.

2. Zero-Day exploit impacts a WordPress Plugin

Description	
Fancy Product Designer, a tool that enables a business to offer customizable products has been identified as vulnerable to critical file upload. The successful exploitation of this vulnerability would allow attackers to upload malware into the sites having the vulnerable plugin installed. A capable remote-based attacker would be able to perform remote code execution of the affected website. The attacker could also leverage gaining complete control of the website. As this plugin has been installed on over 17000 sites, the sites critically at the risk of site takeover. Currently, there has not been any technicality shared about the zero-day exploitation.	
Source	https://www.wordfence.com/blog/2021/06/critical-0-day-in-fancy-product-designer-under-active-attack/
Infected Technology	Fancy Product Designer
Recommendation	Consider updating the plugin to its latest version i.e. 4.6.9.

3. SonicWall Patches Command Injection Flaw in Firewall Management Application

Description	
A vulnerability in the SonicWall NSM On-Prem product allows an authenticated attacker to perform OS command injection using a crafted HTTP request. This vulnerability affects NSM On-Prem 2.2.0-R10 and earlier versions. This critical vulnerability potentially allows a user to execute commands on a device's operating system with the highest system privileges (root). This vulnerability impacts on-premises versions of SonicWall NSM but does not affect NSM SaaS versions.	
Source	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0014
Infected Technology	NSM On-Prem 2.2.0-R10 and earlier versions
CVE ID	CVE-2021-20026
Recommendation	Apply the available patches as soon as possible

4. Siemens Patches Major PLC Flaw that Bypasses Its 'Sandbox' Protection

Description	
SIMATIC S7-1200 and S7-1500 CPU products contain a memory protection bypass vulnerability that could allow an attacker to write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks. A remote unauthenticated attacker with network access to port 102/tcp could potentially write arbitrary data and code to protected memory areas or read sensitive data to launch further attacks.	
Source	https://cert-portal.siemens.com/productcert/pdf/ssa-434534.pdf
Infected Technology	Siemens SIMATIC S7-1200 and S7-1500 PLCs
CVE ID	CVE-2020-15782
Recommendation	Apply the available patches as soon as possible

5. Vulnerability in Lasso Library Impacts Products from Cisco, Akamai

Description	
A high-severity vulnerability discovered recently in an open-source library named Lasso has been found to impact products from Cisco and Akamai, as well as Linux distributions. This vulnerability potentially allows actors with access to a well-formed SAML response for an organization typically authenticated users, but potentially compromised endpoints or malicious proxies to modify their identity and impersonate another user within the same organization. To exploit this issue, the attacker would need to have had a valid credential for an identity provider or have obtained the credentials to authenticate as a valid user. Akamai has now made available technical information about the issue. The company noted that the same vulnerability, known as XML Signature Wrapping, has been reported several times over the past years, and it appears to have existed in the Lasso codebase since 2005.	
Source	https://blogs.akamai.com/2021/06/sogo-and-packetfence-impacted-by-saml-implementation-vulnerabilities.html
Infected Technology	• SOGo and PacketFence packages, • Adaptive Security Appliance (ASA), • Content Security Management Appliance (SMA), • Email Security Appliance (ESA), • FXOS Software, Web Security Appliance (WSA), and • Firepower Threat Defense (FTD) as being affected
CVE ID	CVE-2021-28091
Recommendation	Consider updating to the latest patched version i.e., 2.7.0.

6. Cisco fixed High-Severity issues in Webex, SD-WAN, ASR 5000 software

Description	
Cisco has addressed multiple vulnerabilities in its products, including high-risk flaws in Webex Player, SD-WAN software, and ASR 5000 series software. The IT giant fixed three high-severity vulnerabilities affecting Webex Player for Windows and macOS. Two of them are memory corruption vulnerabilities that impact the Webex Network Recording Player and Webex Player. According to the advisory published by CISCO, it could allow an attacker to execute arbitrary code on an affected system. An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system	
Source	https://tools.cisco.com/security/center/publicationListing.x
Infected Technology	• Webex Player, version 41.4 and later • SD-WAN software • ASR 5000 series software.
CVE ID	CVE-2021-1503, CVE-2021-1526, CVE-2021-1502
Recommendation	Consider applying the security patches released by cisco.

7. Apache Pulsar bug allowed account takeovers in certain configurations

Description	
Server messaging and data exchange platform Apache Pulsar has patched a security bug that could allow an attacker to hijack accounts configured in a specific way. According to the pull request on the Apache Pulsar GitHub reads, if Apache Pulsar is configured to authenticate clients using tokens based on JSON Web Token (JWT), the signature of the token is not validated if the algorithm of the presented token is set to none. This allows an attacker to connect to Pulsar instances as any user (including admins). However, an authenticated user does not directly gain access. It will still go through the authorization process.	
Source	https://seclists.org/oss-sec/2021/q2/163
Infected Technology	Apache Pulsar < 2.7.1
CVE ID	CVE-2021-22160
Recommendation	Consider updating the Apache Pulsar to its latest version i.e. 2.7.1

8. Hackers scan for VMware vCenter servers vulnerable to RCE

Description	
Threat actors are actively scanning the Internet for VMware vCenter servers affected by a critical remote code execution (RCE) vulnerability tracked as CVE-2021-21985. The flaw is caused by the vSphere Client (HTML5) that contains a remote code execution vulnerability due to a lack of input validation in the Virtual SAN Health Check plug-in which is enabled by default in the vCenter Server. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. According to the virtualization giant, a remote attacker can exploit this issue to gain access to vCenter installs exposed online, whether a customer uses vSAN or not.	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0010.html
Infected Technology	vCenter Server 6.5, 6.7, and 7.0
CVE ID	CVE-2021-21985
Recommendation	Consider keeping your system up to date with the patched version.

9. Cisco Discloses Details on macOS SMB Vulnerabilities	
Description	
Cisco's Talos threat intelligence and research unit on Wednesday disclosed the details of several SMB-related vulnerabilities patched recently by Apple in its macOS operating system. Talos disclosed seven vulnerabilities found in SMBX server components and also detailed the process it used to identify them. One of the security holes was fixed silently by Apple, one was addressed in April, and the rest were patched in May. The vulnerabilities are mitigated by the fact that their exploitation requires authentication, but Talos warned that they are readily exploitable in environments with advanced authentication mechanisms. An attacker can exploit the vulnerabilities by sending specially crafted packets to the targeted server.	
Source	https://blog.talosintelligence.com/2021/06/vuln-spotlight-smb-mac-deep-dive.html
Infected Technology	SMBX server components of macOS
Recommendation	Consider applying the security patches released by Apple.

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/