April 26 2021

INFOSEC WEEKLY

#MADE4SECURITY

- 3 Zero-Day Exploits Hit SonicWall Enterprise Email Security Appliances
- Google issues Chrome update patching seven security vulnerabilities
- Critical RCE Bug Found in Homebrew package Manager for macOS and Linux
- Microsoft partially fixes Windows 7, Server 2008 vulnerability
- WordPress 5.7.1 Patches XXE Flaw in PHP 8
- Pulse Secure VPN zero-day used to hack defense firms
- Oracle Delivers 390 Security Fixes with April 2021 CPU

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. 3 Zero-Day Exploits Hit SonicWall Enterprise Email Security Appliances

Description
SonicWall has addressed three critical security vulnerabilities in its hosted and on-premises email security (ES) product. These vulnerabilities were executed in conjunction to obtain administrative access and code execution on a SonicWall ES device. The adversary leveraged these vulnerabilities, with intimate knowledge of the SonicWall application, to install a backdoor, access files, and emails, and move laterally into the victim organization's network. The administrative access not only enabled the attacker to exploit CVE-2021-20023 to read configuration files, counting those containing information about existing accounts as well as Active Directory credentials but also abuse CVE-2021-20022 to upload a ZIP archive containing a JSP-based web shell called BEHINDER that's capable of accepting encrypted command-and-control (C2) communications.

Source	https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/
Infected Technology	SonicWall email Security (ES)
CVE ID	CVE-2021-20021, CVE-2021-20022, CVE-2021-20023
Recommendation	Apply the Updates to latest versions

2. Google issues Chrome update patching seven security vulnerabilities

Description
Google on Wednesday released version 90.0.4430.85 of the Chrome browser for Windows, Mac, and Linux. The release contains seven security fixes, including one for a zero-day vulnerability that was exploited in the wild. The zero-day, which was assigned the identifier of CVE-2021-21224, was described as a “type confusion in V8”. The other five vulnerabilities were detailed as CVE-2021-21222 heap buffer overflow in v8, a CVE-2021-21223 integer overflow in Mojo, CVE-2021-21225 out of bounds memory access in V8, CVE-2021-21226 use after free in navigation, and CVE-2021-21224 type confusion in V8.

Source	https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_20.html
Infected Technology	Chrome browser
CVE ID	CVE-2021-21224, CVE-2021-21223, CVE-2021-21225, CVE-2021-21226, CVE-2021-21224
Recommendation	Consider upgrading Chrome to the latest patched version.

3. Critical RCE Bug Found in Homebrew package Manager for macOS and Linux

Description

A recently identified security vulnerability in the official Homebrew Cask repository could have been exploited by an attacker to execute arbitrary code on users' machines that have Homebrew installed. According to Homebrew's Markus Reiter, the discovered vulnerability would allow an attacker to inject arbitrary code into a cask and have it be merged automatically. This is due to a flaw in the *git_diff* dependency of the *review-cask-pr* GitHub Action, which is used to parse a pull request's diff for inspection. Due to this flaw, the parser can be spoofed into completely ignoring the offending lines, resulting in successfully approving a malicious pull request." Also, if this vulnerability was abused by a malicious actor, it could be used to compromise the machines that run brew before it gets reverted.

Source	https://brew.sh/2021/04/21/security-incident-disclosure/
Infected Technology	Homebrew Package Manager
Recommendation	Consider using the alternative of Homebrew until the vulnerability gets patched.

4. Microsoft partially fixes Windows 7, Server 2008 vulnerability

Description

Microsoft has issued a partial fix (micropatch) for a local privilege escalation (LPE) vulnerability impacting all Windows 7 and Server 2008 R2 devices. This LPE vulnerability (not yet officially tracked using a CVE ID) stems from the misconfiguration of two service registry keys and it allows local attackers to escalate privileges on any fully patched systems. The insecure permissions on the registry keys of the RpcEptMapper and DnsCache services enable attackers to trick the RPC Endpoint Mapper service to load malicious DLLs on Windows 7 and Windows Server 2008R2. By exploiting this issue, attackers can execute arbitrary code in the context of the Windows Management Instrumentation (WMI) service that runs with Local System permissions.

Source	https://itm4n.github.io/windows-registry-rpceptmapper-eop/
Infected Technology	Windows 7 and Server 2000 R2 devices
Recommendation	Consider applying micropatch until Microsoft fully patches the vulnerability

5. WordPress 5.7.1 Patches XXE Flaw in PHP 8

Description	
WordPress has released version 5.7.1 of its popular content management system (CMS), which brings more than 25 bug fixes, including patches for two security vulnerabilities. One of the patched security flaws is an XML External Entity (XXE) vulnerability in the ID3 library in PHP 8, which is used by WordPress. Designed to parse ID3 tags from MP3 audio files, the library did not explicitly disable XML entities in PHP 8, which rendered WordPress 5.7 and older versions vulnerable to XXE attacks via MP3 file uploads. The issue could be exploited by any user who can upload files. Only WordPress deployments that use PHP 8 (0.3%) are affected.	
Source	https://wordpress.org/news/2020/04/wordpress-5-4-1/
Infected Technology	WordPress
CVE ID	CVE-2021-29447
Recommendation	Upgrade the content management system (CMS) to version 5.7.1

6. Pulse Secure VPN zero-day used to hack defense firms

Description	
A vulnerability was discovered under Pulse Connect Secure (PCS). This includes an authentication by-pass vulnerability that can allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway. This vulnerability has a critical CVSS score and poses a significant risk. Pulse Secure has shared mitigation measures for the zero-day vulnerability in the Pulse Connect Secure (PCS) SSL VPN appliance actively exploited in attacks against worldwide organizations and focused on US Defense Industrial Base (DIB) networks.	
Source	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784
Infected Technology	Pulse Connect Secure VPN
CVE ID	CVE-2021-22893
Recommendation	upgrade the Pulse Connect Secure server software version to the 9.1R.11.4

7. Oracle Delivers 390 Security Fixes with April 2021 CPU

Description

Oracle this week announced the release of 390 new security fixes as part of the April 2021 Critical Path Update (CPU), including patches for more than 200 bugs that could be exploited remotely without authentication. Oracle's E-Business Suite received patches for the largest number of security holes, namely 70. Of these, 22 could be exploited remotely by unauthenticated attackers. MySQL was also highly impacted, with patches for 49 vulnerabilities, 10 of which could be exploited remotely without authentication. Fusion Middleware and Retail Applications also received fixes for a large number of security issues, namely 45 (36 remotely exploitable without authentication) and 33 (31 exploitable by remote, unauthenticated attackers). Other Oracle products that received patches include ZFS Storage Appliance Kit, Cloud Infrastructure Storage Gateway, and Storage Cloud Software Appliance.

Source	https://www.oracle.com/security-alerts/cpuapr2021.html
Infected Technology	Oracle-based products
CVE ID	CVE-2021-2177, CVE-2021-2248, CVE-2020-1472, CVE-2021-2317, CVE-2021-2256
Recommendation	Consider reviewing Oracle's quarterly patches and apply necessary software updates as soon as possible

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/