May 31
2021

INFOSEC WEEKLY

#MADE4SECURITY

- VMware vCenter Server vulnerable to Remote Code Execution
- VSCode Extension Bugs Could Lead to Supply Chain Attacks
- Apple fixes three zero-days, one abused by XCSSET macOS malware
- Wormable Windows HTTP vulnerability also affects WinRM servers
- Details Disclosed on Critical Flaws Affecting Nagios IT Monitoring Software
- Thousands of Chrome extensions are tampering with security headers
- Google Patches 32 Vulnerabilities with Release of Chrome 91
- SonicWall fixes an NSM On-Prem bug, patch it ASAP
- HPE fixes critical zero-day vulnerability disclosed in December

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. VMware vCenter Server vulnerable to Remote Code Execution

Description	
VMware has announced patches in the vCenter Server lineup. The vCenter server had a critical security vulnerability that will let a remote-based attacker execute arbitrary command upon successful exploitation. VMware vCenter Server is a management utility that controls virtual machines, ESXi hosts and other components into a single centralized location. The malicious attacker would exploit the issue within it by gaining network access to port 443. The attacker would then execute commands with unrestricted privileges on the underlying operating system that hosts the vCenter Server.	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0010.html
Infected Technology	VCenter Server 6.5, 6.7, 7.0 Cloud Foundation 3.x, 4.x
CVE ID	CVE-2021-21985
Recommendation	Install the latest security patch released by VMware

2. VSCode Extension Bugs Could Lead to Supply Chain Attacks

Description	
Visual Studio (VS) Code extensions are identified as severe security flaws. The flaws within the extensions enable a malicious actor to compromise local machine, build and deployment systems via the developer's integrated development environment (IDE). The vulnerable extension lets an attacker execute arbitrary code on the affected system remotely. The attacker could also execute multiple tasks for enabling supply chain attacks. The vulnerable extensions have a cumulative installation count of about two million. Some of the vulnerable extension names are: 'LaTeX Workshop', 'Rainbow Fart', Instant Markdown', and 'Open in Default Browsers'. The flaws within the extensions have been addressed.	
Source	https://snyk.io/blog/visual-studio-code-extension-security-vulnerabilities-deep-dive/
Infected Technology	Microsoft Visual Studio Code
Recommendation	Consider installing the extensions only from trusted sources.

3. Apple fixes three zero-days, one abused by XCSSET macOS malware

Description	
Apple has released security updates to patch three macOS and tvOS zero-day vulnerabilities attackers exploited in the wild, with the former being abused by the XCSSET malware to bypass macOS privacy protections. Two of the three zero-days impact WebKit on Apple TV 4K and Apple TV HD devices. Threat actors could exploit the two vulnerabilities using maliciously crafted web content that would trigger arbitrary code execution on unpatched devices due to a memory corruption issue. The third zero-day impacts macOS Big Sur devices, and it is a permission issue found in the Transparency, Consent, and Control (TCC) framework. Attackers could exploit this vulnerability using a maliciously crafted application that may bypass Privacy preferences and access sensitive user data.	
Source	https://www.jamf.com/blog/zero-day-tcc-bypass-discovered-in-xcsset-malware/
Infected Technology	macOS and tvOS
CVE ID	CVE-2021-30663, CVE-2021-30665 and CVE-2021-30713
Recommendation	Apply the patch as soon as possible

4. Wormable Windows HTTP vulnerability also affects WinRM servers

Description	
A wormable vulnerability in the HTTP Protocol Stack of the Windows IIS server can also be used to attack unpatched Windows 10 and Server systems publicly exposing the WinRM (Windows Remote Management) service. Microsoft already patched the critical bug tracked as CVE-2021-31166 during the May Patch Tuesday. Luckily, although it can be abused by threat in remote code execution (RCE) attacks, the vulnerability ONLY impacts versions 2004 and 20H2 of Windows 10 and Windows Server. The bug was found in the HTTP Protocol Stack (HTTP.sys) used as a protocol listener by the Windows IIS web server for processing HTTP requests.	
Source	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31166
Infected Technology	Windows 10 and Windows Server
CVE ID	CVE-2021-31166
Recommendation	Apply the patches as soon as possible

5. Details Disclosed on Critical Flaws Affecting Nagios IT Monitoring Software

Description

Cybersecurity researchers disclosed details about 13 vulnerabilities in the Nagios network monitoring application that could be abused by an adversary to hijack the infrastructure without any operator intervention. The issues, which consist of a mix of authenticated remote code execution (RCE) and privilege escalation flaws, were discovered and reported to Nagios in October 2020, following which they were remediated in November. Chief among them is CVE-2020-28648 (CVSS score: 8.8), which concerns an improper input validation in the Auto-Discovery component of Nagios XI that the researchers used as a jumping-off point to trigger an exploit chain that strings together a total of five vulnerabilities to achieve a "powerful upstream attack."

Source	https://skylightcyber.com/2021/05/20/13-nagios-vulnerabilities-7-will-shock-you/
Infected Technology	Nagios IT Monitoring Software
CVE ID	CVE-2020-28648, CVE-2020-28900, CVE-2020-28901, CVE-2020-28902, CVE-2020-28903, CVE-2020-28904, CVE-2020-28905, CVE-2020-28906, CVE-2020-28907, CVE-2020-28908, CVE-2020-28909, CVE-2020-28910,
Recommendation	Update the software to its latest versions

6. Thousands of Chrome extensions are tampering with security headers

Description

Thousands of Google Chrome extensions available on the official Chrome Web Store are tampering with security headers on popular websites, putting users at risk of a wide range of web-based attacks. According to CISPA Helmholtz Center for Information Security, 2,485 extensions were found intercepting and modifying at least one security used by todays' Top 100 most popular websites like Content-Security-Policy (CSP), HTTP Strict-Transport-Security (HSTS), X-Frame-Options, and X-Content-Type-Options. According to the research team, if the extensions want to enrich a users' experience online by tampering with security headers, all the extensions can be used to expose the users to attacks from other scripts and sites running inside the browser and on the web.

Source	https://madweb.work/preprints/madweb21-paper16-pre_print_version.pdf/
Infected Technology	Google Chrome extensions
Recommendation	Consider validating security headers of your website.

7. Google Patches 32 Vulnerabilities with Release of Chrome 91

Description

Google on Tuesday announced the release of Chrome 91 to the stable channel. The latest update patches a total of 32 vulnerabilities. Of the addressed issues, 21 vulnerabilities were discovered by external researchers, including 8 high-severity bugs, 8 medium-severity flaws, and 5 low-severity security holes. The most important of these is a heap buffer overflow in Autofill, for which Google paid a $20,000 bounty reward to the reporting researcher. The new browser release also includes patches for six high-severity use-after-free flaws in WebAudio, WebRTC, TabStrip, TabGroups, WebUI, and WebAuthentication. The eighth high-risk security bug is an out-of-bounds write in TabStrip. Four of the eight medium-severity issues addressed with this Chrome update are insufficient policy enforcements.

Source	https://chromereleases.googleblog.com/2021/05/stable-channel-update-for-desktop_25.html
Infected Technology	Google Chrome Browser
CVE ID	CVE-2021-30521
Recommendation	Consider updating to the latest patched version.

8. SonicWall fixes an NSM On-Prem bug, patch it ASAP

Description

SonicWall urges customers to ‘immediately’ address a post-authentication vulnerability, impacting on-premises versions of the Network Security Manager (NSM). The flaw could be exploited by an attacker to perform OS command injection using a crafted HTTP request. The flaw affects NSM version 2.2.0-R10-H1 and earlier, the security vendor addressed it with the release of NSM 2.2.1-R6 and 2.2.1-R6 (Enhanced) versions According to SonicWall, this critical vulnerability potentially allows a user to execute commands on a device’s operating system with the highest system privileges (root).

Source	https://www.sonicwall.com/support/product-notification/security-advisory-on-prem-sonicwall-network-security-manager-nsm-command-injection-vulnerability/210525121534120/
Infected Technology	SonicWall’s NSM version 2.2.0-R10-H1 and earlier.
CVE IDs	CVE-2021-20026
Recommendation	Consider updating the NSM to its latest version.

9. HPE fixes critical zero-day vulnerability disclosed in December

Description	
HPE-SIM is remote support automation and management solution for HPE servers, storage, and networking products, including HPE's ProLiant Gen10 and ProLiant Gen9 servers. It has released a security update to address a zero-day remote code execution vulnerability in the HPE Systems Insight Manager (SIM) software, disclosed last year, in December. The RCE vulnerability was found in the latest versions (7.6.x) of HPE's proprietary Systems Insight Manager (SIM) software, and it ONLY affects the Windows version. HPE rated the bug as a critical severity security flaw as it allows attackers with no privileges to exploit it in low complexity attacks that don't require user interaction.	
Source	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04068en_us
Infected Technology	HPE Systems Insight Manager (SIM) software
CVE IDs	CVE-2020-7200
Recommendation	Consider applying the security patches released by HPE.

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/