May 03
2021

INFOSEC WEEKLY

#MADE4SECURITY

- macOS computers affected due to a 0-Day Gatekeeper Flaw
- F5 BIG-IP vulnerable to Kerberos KDC Spoofing
- Command injection flaw in PHP Composer allowed supply-chain attacks
- FBI, CISA Uncover Tactics Employed by Russian Intelligence Hackers
- Microsoft finds critical code execution bugs in IoT, OT devices
- Google Patches Yet Another Serious V8 Vulnerability in Chrome
- Linux Kernel Bug Opens Door to Wider Cyberattacks
- Several High-Severity Vulnerabilities Expose Cisco Firewalls to Remote Attacks

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. macOS computers affected due to a 0-Day Gatekeeper Flaw

Description

Apple has released an update to the macOS operating system addressing an exploited zero-day vulnerability. The vulnerability allowed attackers to avoid all the security protection implemented by the OS to permit unapproved software to run on. Gatekeeper is a feature within the macOS allowing only the trusted applications to run within the OS environment. This feature ensures the authenticity of the app from a registered developer or the App Store. The vulnerability present within this feature allowed attackers to manipulate the search engines and send malicious links to redirect the users to the sites and perform an automated download. The software download was possible using bash scripting that retrieved next-stage payloads including adware.

Source	https://support.apple.com/en-us/HT212325
Infected Technology	Apple macOS
CVE ID	CVE-2021-30657
Recommendation	Consider installing the security patch released by Apple.

2. F5 BIG-IP vulnerable to Kerberos KDC Spoofing

Description

A bypass vulnerability has been identified in the Kerberos Key Distribution Center (KDC) security feature that impacts the F5 Big-IP application delivery services. The vulnerability allowed attackers to bypass Kerberos authentication, security policies and gain unauthorized access to the sensitive workloads of the Big-IP Access Policy Manager (APM). The bypass authentication is also present in the Big-IP admin console. A remote-based attacker can hijack the KDC connection using spoofed AS-REP responses. The spoofed credentials would fail in the authentication token validation however, the spoofed credential regarding this vulnerability could lead to local administrative access for an administrative user using the APM access policy.

Source	https://support.f5.com/csp/article/K51213246
Infected Technology	BIG IP ARM 12.1.6, 13.1.4, 14.1.4 and 15.1.3
CVE ID	CVE-2021-23008
Recommendation	Consider updating the system as soon as the patch is released by F5.

3. Command injection flaw in PHP Composer allowed supply-chain attacks

Description	
The maintainers of the PHP Composer package have addressed a critical vulnerability, tracked as CVE-2021-29472, that could have allowed an attacker to execute arbitrary commands and establish a backdoor in every PHP package. A vulnerability in such a central component, serving more than 100M package metadata requests per month, has a huge impact as this access could have been used to steal maintainers' credentials or to redirect package downloads to third-party servers delivering backdoored dependencies.	
Source	https://blog.sonarsource.com/php-supply-chain-attack-on-composer
Infected Technology	PHP Composer
CVE ID	CVE-2021-29472
Recommendation	Immediately update Composer to version 2.0.13 or 1.10.22

4. FBI, CISA Uncover Tactics Employed by Russian Intelligence Hackers

Description	
The U.S. Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) on Monday published a new joint advisory as part of their latest attempts to expose the tactics, techniques, and procedures (TTPs) adopted by the Russian Foreign Intelligence Service (SVR) in its attacks targeting the U.S and foreign entities. The SVR activity—which includes the recent SolarWinds Orion supply chain compromise—primarily targets government networks, think tank and policy analysis organizations, and information technology companies and seeks to gather intelligence information.	
Source	https://us-cert.cisa.gov/ncas/current-activity/2021/04/26/fbi-dhs-cisa-joint-advisory-russian-foreign-intelligence-service
Recommendation	Review Joint CSA AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders and implement the recommended mitigations.

5. Microsoft finds critical code execution bugs in IoT, OT devices

Description	
Microsoft security researchers have discovered over two dozen critical remote code execution (RCE) vulnerabilities in Internet of Things (IoT) devices and Operational Technology (OT) industrial systems. These 25 security flaws are known collectively as BadAlloc and are caused by memory allocation Integer Overflow or Wraparound bugs. Threat actors can exploit them to trigger system crashes and execute malicious code remotely on vulnerable IoT and OT systems. The vulnerabilities were found by Microsoft's researchers in standard memory allocation functions widely used in multiple real-time operating systems (RTOS), C standard library (libc) implementations, and embedded software development kits (SDKs).	
Source	https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04
Infected Technology	Internet of Things (IoT) devices and Operational Technology (OT) industrial system
Recommendation	Consider applying the security patches released by Vendor.

6. Google Patches Yet Another Serious V8 Vulnerability in Chrome

Description	
An update released this week by Google for Chrome v90 patches yet another serious vulnerability affecting the V8 JavaScript engine used by the web browser. The flaw was initially reported to Google by researcher Gengming Liu who claimed that the flaw could be exploited for remote code execution in the targeted user’s browser. Including, in recent weeks, Google has patched several serious V8 vulnerabilities which contained few high-severity issues, three medium-severity bugs, and one low-severity vulnerability, most of whose PoC exploits were released before patches were made available. Hence, for some of these vulnerabilities, Google has warned that exploits may still exist in the wild.	
Source	https://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop_26.html
Infected Technology	Google Chrome Web Browser
CVE ID	CVE-2021-21227
Recommendation	Consider updating the Google Chrome Browser.

7. Linux Kernel Bug Opens Door to Wider Cyberattacks

Description

An information disclosure security vulnerability has been discovered in the Linux kernel, which can be exploited to expose information in the kernel stack memory of vulnerable devices. Specifically, the bug exists in the /proc/pid/syscall functionality of 32-bit ARM devices running Linux, according to Cisco Talos. It arises from an improper conversion of numeric values when reading the file. With only a few commands, attackers can output 24 bytes of uninitialized stack memory, which can be used to bypass kernel address space layout randomization (KASLR). If utilized correctly, attacks would be impossible to detect on a network remotely. Also, they could leverage this information leak to successfully exploit additional unpatched Linux vulnerabilities.

Source	https://blog.talosintelligence.com/2021/04/vuln-spotlight-linux-kernel.html
Infected Technology	32-bit ARM devices running Linux
CVE ID	CVE-2020-28588
Recommendation	Consider updating to the patched Linux Kernel versions: 5.10-rc4, 5.4.66, and 5.9.8

8. Several High-Severity Vulnerabilities Expose Cisco Firewalls to Remote Attacks	
Description	
Cisco this week released patches for multiple vulnerabilities in Firepower Threat Defense (FTD) software, including high-severity issues that could be exploited for arbitrary command execution or denial-of-service (DoS) attacks. The first one is the command injection bug which an attacker can abuse to execute arbitrary commands as root on the underlying OS. This flaw exists because user-supplied command arguments aren't sufficiently validated. Another flaw rooted in insufficient validation impacts the software-based SSL/TLS message handler of FTD and could be abused to cause a DoS. Besides, unauthenticated attackers could exploit this vulnerability by sending a "crafted SSL/TLS message" through an affected device. Likewise, four other DoS bugs addressed this week in FTD also impact Cisco Adaptive Security Appliance (ASA) software and could all be exploited remotely.	
Source	https://tools.cisco.com/security/center/publicationListing.x
Infected Technology	Firepower 4100/9300 series, ISA 3000 series, ASA 5512-X, ASA 5515-X, ASA 5545-X, ASA 5555-X
CVE ID	CVE-2021-1448, CVE-2021-1402, CVE-2021-1445, CVE-2021-1504, CVE-2021-1501
Recommendation	Consider installing the available patches 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/