January 17, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Millions of Routers Exposed to RCE by USB Kernel Bug
- Undetected SysJoker Backdoor Malware Targets Windows, Linux & MacOS
- Microsoft Patch Released to fix Critical 'Wormable' Windows Vulnerability
- Researchers Found Dozen over Bugs in Widely Used URL Parsers Libraries
- Millions of Vulnerable Versions of Log4j Have Been Downloaded Over the Past Month
- WordPress 5.8.3 Security Update Released

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.

Millions of Routers Exposed to RCE by USB Kernel Bug

Description

Millions of popular routers are at risk of remote code execution (RCE) due to a high-severity flaw in the KCodes NetUSB Kernel module. The module uses the proprietary NetUSB protocol that enables remote devices to connect to routers over IP and access any USB devices that are plugged into them and Linux kernel driver that launches a server, which makes the USB devices available via the network. Based on the writeup from SentinelOne vulnerability researcher, attackers could remotely exploit the vulnerability to execute code in the kernel via a pre-authentication buffer overflow security vulnerability, allowing device takeover.

Source	https://threatpost.com/millions-routers-exposed-bug-usb-module-kcodes-netusb/177506/
Infected Technology	KCodes NetUSB Kernel Module Based Vendor Routers.
Recommendation	• Updating the firmware with the latest patch attached for each specific vendor.

Undetected SysJoker Backdoor Malware Targets Windows, Linux & MacOS

Description

Researchers have warned a new multiplatform malware distributes via malicious npm packages, is spreading under the radar with Linux and Mac versions going fully undetected in VirusTotal. In Windows version, has only six detections as of this writing. The backdoor is used for establishing initial access on a target machine. Once installed it, can execute code as well as additional commands, through which malicious actors can carry out system commands or pivot to move further into a corporate network. This kind of initial access is on the eye of underground cyberforums, ransomware and others can purchase it.

Source	https://threatpost.com/millions-routers-exposed-bug-usb-module-kcodes-netusb/177506/
Infected Technology	Multiplatform Devices like Windows, Linux, Mac OS
Recommendation	• Users or admins can first use memory scanners to detect a SysJoker payload in memory. • They can also use detection content to search endpoint detection and response (EDR) and security information and event management (SIEM) platforms.

Microsoft Patch Released to fix Critical 'Wormable' Windows Vulnerability

Description	
Microsoft released update on Tuesday by plugging 96 security holes across it system, urging customers to prioritize patching for a critical "Wormable" vulnerability. Out of 96 vulnerabilities, nine are rated Critical and 89 are rated important in severity with six zero-day publicly known at the time of release. Among all vulnerabilities CVE-2022-21907, a remote code execution vulnerability rooted in HTTP Protocol Stack is major one. According to Russian security researcher Mikhail Medvedev, that it's wormable, meaning no user interaction is necessary to trigger and propagate the infection.	
Source	https://thehackernews.com/2022/01/first-patch-tuesday-of-2022-brings-fix.html
Infected Technology	Microsoft Windows Server 2019 and Windows 10 version 1809.
Recommendation	• Applying the patch released by Microsoft to fix 96 security holes.
CVE_ID	CVE-2022-21907

Researchers Found Dozen over Bugs in Widely Used URL Parsers Libraries

Description

The inconsistencies and confusions in 16 different URL parsing libraries could be exploited to bypass validations and open door to a wide range of attack vectors. In deep analysis conducted by cybersecurity firms Claroty and Synk, eight security vulnerabilities were identified in as many third-party libraries written in different languages as C, JavaScript, PHP, Python and Ruby which are used by several web applications. According to the report shared by a researcher with The Hacker News, threat actors can perform attacks to cause denial-of-service conditions, information leaks, or possibly remote code execution due to confusion and unexpected behavior in URL parsing libraries.

Source	https://thehackernews.com/2022/01/researchers-find-bugs-in-over-dozen.html?m=1
Infected Technology	16 URL parsing Libraries written in Different languages such as C, java, PHP, Python, Ruby.
Recommendation	To protect applications from URL parsing vulnerabilities: • Use as few parsers as possible • Understand differences in parsers involved with application logic. • Also, patching the vulnerability with the released patch for each specific parser.
CVE_ID	CVE-2021-33056, CVE-2021-23414, CVE-2021-37352, CVE-2021-23385, CVE-2021-32618, CVE-2021-23393, CVE-2021-23401, CVE-2021-23435

Millions of Vulnerable Versions of Log4j Have Been Downloaded Over the Past Month

Description	
Sonatype, the company that runs Apache Maven's Central Repository, claims that vulnerable versions of Log4j have been downloaded four million times since December 10. It is unclear why there is such a high number of vulnerable downloads. Sonatype also noted that approximately 40% of Log4j downloads over the weekend were of the most recent versions. If the CI processes are downloading libraries on a regular basis, ensure that they are downloading the most recent approved versions. Verify that you've qualified the upgraded versions, such as Log4j 2.17.1.	
Source	https://www.theregister.com/2022/01/11/outdated_log4j_downloads/
Infected Technology	Apache Software Foundation Log4j Library
Recommendation	• Verifying the downloaded library is most recent approved version.

WordPress 5.8.3 Security Update Released

Description	
The WordPress 5.8.3 Security Release includes fixes for four vulnerabilities: two SQL injection, one cross-site scripting, and one admin object injection. The vulnerabilities affect WordPress versions from 3.7 to 5.8. Among those four vulnerabilities, three are rated as high severity. If auto-update is enabled by default, these vulnerabilities have been patched via the automated update. If not, the patch can be installed by simply updating via the administrator dashboard.	
Source	https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/
Infected Technology	WordPress versions between 3.7 and 5.8
Recommendation	• Update to latest WordPress Released Version
CVE_ID	CVE-2022-21661, CVE-2022-21662, CVE-2022-21663 and CVE-2022-21664

New Unpatched Apple Safari Browser Bug Allows Cross-Site User Tracking

Description

A software bug introduced in Apple Safari 15's implementation of the IndexedDB API could be abused by a malicious website to track users' online activity in the web browser and worse, even reveal their identity. The vulnerability, dubbed IndexedDB Leaks, was disclosed by fraud protection software company FingerprintJS, which reported the issue to the iPhone maker on November 28, 2021. Like most web storage solutions, IndexedDB follows a same-origin policy. In Safari 15 on macOS, and in all browsers on iOS and iPadOS 15, the IndexedDB API is violating the same-origin policy. Every time a website interacts with a database, a new (empty) database with the same name is created in all other active frames, tabs, and windows within the same browser session. A consequence of this privacy violation is that it allows websites to learn what other websites a user is visiting in different tabs or windows, not to mention precisely identify users on Google services services like YouTube and Google Calendar as these websites create IndexedDB databases that include the authenticated Google User IDs, which is an internal identifier that uniquely identifies a single Google account.

Source	https://thehackernews.com/2022/01/new-unpatched-apple-safari-browser-bug.html?m=1
Infected Technology	Apple Safari Browser.
Recommendation	Temporarily switch to another browser to avoid their data leaking across origins.

Microsoft Released Windows Server Updates due to critical bugs

Description

Admins who installed Microsoft's Windows Server patches this week began reporting a slew of serious issues shortly after they were released. Domain controllers went into an unending reboot loop, ReFS volumes became inaccessible and appeared as RAW file systems, and Hyper-V no longer started on servers. Microsoft has withdrawn the January Windows Server upgrades, and they are no longer available through Windows Update. Affected versions of Windows Servers may restart abruptly after installing KB5009557 on domain controllers (DCs). When DCs use Shadow Principals in Enhanced Security Admin Environment (ESAE) or environments with Privileged Identity Management (PIM), you are more likely to be affected on Windows Server 2016 and later, Microsoft has also acknowledged that they are looking into a problem where "virtual machines (VMs) in Hyper-V can fail to start" while applying upgrades on UEFI devices.

Source	https://www.bleepingcomputer.com/news/microsoft/microsoft-pulls-new-windows-server-updates-due-to-critical-bugs/
Infected Technology	Window Server 2012, window Server 2019 & Window Server 2022.
Recommendation	Do not install recent Microsoft Updates.

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/