

November 14, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Microsoft warns of Uptick in hackers leveraging publicly disclosed 0-Day Vulnerabilities
- New UEIF Firmware Flaws Reported in Several Lenovo Notebook Models
- New Privilege Escalation vulnerability in Linux Operating System's kernel.
- Multiple critical flaws affect widely used OpenLiteSpeed web server software.
- Citrix Issues Patches for Critical Flaw Affecting ADC and Gateway Products.



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.

Microsoft warns of Uptick in hackers leveraging publicly disclosed o-Day Vulnerabilities

Description

Cybercriminal is taking the full advantage of publicly disclosed zero-day vulnerability for breaching the targeted websites. In the report of Digital Defense Report by tech giant, they mentioned that the time between the time of vulnerability exposed, and use of that vulnerability is decreasing. Thus, the organization who are using those services must take immediate action to the threat and must be updated with the release of these zero-day vulnerability. According to the CISA Cybersecurity Infrastructure Security Agency found that the attacker is aggressively targeting and attacking newly disclosed software bugs. This case is very critical as once the vulnerability is exposed by the threat actors, the other threat actors misuse the vulnerability for exploiting another nation as zero-day attacks are quickly executed before the patches are installed by that organization.

Source <https://thehackernews.com/2022/11/microsoft-warns-of-uptick-in-hackers.html>

Infected Technology Vulnerable servers and its software.

Recommendation • Patch the vulnerable system or monitor the vulnerability for possible exploitation.

CVE_ID
CVE-2021-35211
CVE-2021-40539
CVE-2021-44077
CVE-2021-42321
CVE-2022-26134

New UEFI Firmware Flaws Reported in Several Lenovo Notebook Models

Description

Since the beginning of the year, Lenovo has corrected this set of three flaws in the Unified Extensible Firmware Interface (UEFI) firmware three times. The flaws make it feasible for threat actors to execute malicious boot loaders, giving the attackers privileged access to the compromised hosts, by deactivating UEFI Secure Boot or restoring factory default Secure Boot databases all from an OS. As a result, it is possible for an adversary to exploit the weaknesses, which are designated CVE-2022-3430, CVE-2022-3431, and CVE-2022-3432, to disable Secure Boot, a security feature intended to stop malicious applications from loading during the boot process.

Source	https://thehackernews.com/2022/11/new-uefi-firmware-flaws-reported-in.html
--------	---

Infected Technology	Unified Extensible Firmware Interface
---------------------	---------------------------------------

Recommendation	<ul style="list-style-type: none">• Update their firmware to the latest version as soon as possible.
----------------	--

CVE_ID	CVE-2022-3430 CVE-2022-3431 CVE-2022-3432
--------	---

New Privilege Escalation vulnerability in Linux Operating System's kernel.

Description

Redhat issued a risk notice for linux kernel local privilege escalation vulnerability, the vulnerability number CVE-2022-3997. This flaw is use-after-free bug that was found in the mctp_sk_unhash in linux kernel net/mctp/af_mctp.c. the reason for the bug is that the simultaneous DROPTAG ioctl and socket close may lead to race condition.

Source	https://securityonline.info/cve-2022-3977-linux-kernel-local-privilege-escalation-vulnerability/
--------	---

Infected Technology	Linux Endpoints
---------------------	-----------------

Recommendation	<ul style="list-style-type: none">• Update to the latest version of the Operating system as soon as possible.
----------------	---

CVE_ID	CVE-2022-3977
--------	---------------

Multiple critical flaws affect widely used OpenLiteSpeed web server software.

Description

Vulnerabilities have been found in the OpenLiteSpeed Web Server and its enterprise version that might be exploited to allow remote code execution. Palo Alto Networks Unit 42 stated that attackers could take control of the web server by connecting and exploiting the vulnerabilities. With 1.9 million distinct servers worldwide, OpenLiteSpeed ranks as the sixth most popular web server. Accessing restricted files in the web root directory could be made possible by a directory traversal vulnerability. The final two flaws involve command injection and privilege escalation. After a responsible disclosure on October 4, 2022, the problems have been fixed in versions 1.7.16 and 6.0.12.

Source	https://thehackernews.com/2022/11/multiple-high-severity-flaw-affect.html
--------	---

Infected Technology	OpenLiteSpeed Web Server & it's enterprise version.
---------------------	---

Recommendation	<ul style="list-style-type: none">• Update to the latest version of the Operating system as soon as possible.
----------------	---

CVE_ID	CVE-2022-0073 CVE-2022-0074
--------	--------------------------------

Citrix Issues Patches for Critical Flaw Affecting ADC and Gateway Products.

Description

A critical authentication bypass problem in the application delivery controller (ADC) and Gateway products, which could be used to take over vulnerable computers, has been fixed by Citrix through the deployment of security upgrades. A successful exploitation in the settings have allowed an attacker to bypass login brute-force protections, take control of a remote desktop, and get authorized access. Customers depending on cloud services directly controlled by Citrix are not required to carry any action, according to the cloud computing and virtualization technology provider.

Source	https://thehackernews.com/2022/11/citrix-issues-patches-for-critical-flaw.html
--------	---

Infected Technology	Application delivery controller (ADC) and Gateway
---------------------	---

Recommendation	<ul style="list-style-type: none">• It is recommended that affected users of Citrix ADC and Citrix Gateway install the relevantly updated versions of those products as possible.
----------------	---

CVE_ID	CVE-2022-27516.
--------	-----------------

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/>