November 02, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- WordPress patched 3-Year old High severity RCE Bug
- Google discloses Windows 0-day exploited in the wild
- NVIDIA patches Critical vulnerability affecting High performance servers
- Multiple vulnerabilities in Synology SRM
- Oracle WebLogic Server RCE Flaw Under Active Attack
- Browser Bugs exploited to install backdoors on computers

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. WordPress patched 3-Year old High severity RCE Bug

Description	
WordPress released a new update for its web publishing software platform. The update includes patch for high severity RCE bug which allows remote unauthenticated attacker to take over system hosting vulnerable website. The vulnerability exists due to improper management of internal resources within application. The flaw can leverage denial of service into RCE. The update also contains four medium severity vulnerability. The medium severity flaw include Cross-site scripting, improper access control, cross site request forgery and security restriction bypass where the first three can be exploited by remote unauthenticated user.	
Source	https://wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance-release/
Infected Technology	WordPress 5.5.1 and earlier
Recommendation	Update to the newer version

2. Google discloses Windows 0-day exploited in the wild

Description	
Researcher from Google have disclosed a 0-dat vulnerability in Windows OS that is being actively exploited. The vulnerability was used together with another Chrome 0-day that has been patched recently. The Chrome bug was used to allow attacker to run malicious code inside Chrome which combine with Window's vulnerability allowed attacker to escape Chrome's security container and run code in underlying OS. The vulnerability is known as Sandbox escape. The flaw resides in Windows kernel affecting Windows 7 to most of recent Windows 10 release. The flaw was patched in newer version of Chrome and expected to be fixed in this week's Microsoft update.	
Source	https://bugs.chromium.org/p/project-zero/issues/detail?id=2104
Infected Technology	Windows 10 Google Chrome
CVE	CVE-2020-17087 CVE-2020-15999
Recommendation	Update to the latest release of Chrome Apply the update for fixation after Microsoft releases the update

3. NVIDIA patches Critical vulnerability affecting High performance servers

Description	
NVIDIA released a patch for critical bugs in its high-performance line of DGX servers. The flaw allowed remote attacker to take control of and access sensitive data on systems. The patch is part of nine patches released for NVIDIA's firmware that runs of DGX AMI baseboard management controller (BMC). The vulnerable module is used for remote monitoring service servers. NVIDIA also informed that a patch for one high-severity bug residing as a hard-coded RSA 1024 key with weak cipher will not be fixed until 2021. The same flaw for server excluding DGX A100 server line has been released.	
Source	https://nvidia.custhelp.com/app/answers/detail/a_id/5010
Infected Technology	NVIDIA DGX Servers
CVE	CVE-2020-11483, CVE-2020-11484, CVE-2020-11485, CVE-2020-11486, CVE-2020-11487, CVE-2020-11488, CVE-2020-11489, CVE-2020-11615, CVE-2020-11616
Recommendation	Update the patches released by NVIDIA Apply the workaround for unfixed vulnerability

4. Multiple vulnerabilities in Synology SRM

Description	
Recently discovered multiple remote vulnerabilities by Cisco Talos in software that helps power Synology routers. The bugs exist in Synology Router Manager (SRM) — a Linux-based operating system for Synology routers — and QuickConnect, a feature inside SRM that allows users to remotely connect to their routers. An adversary could use these vulnerabilities to carry out a range of malicious actions, including executing remote code on the device, the exposure of sensitive information regarding the victim's network and communication with other devices connected to the same network.	
Source	https://blog.talosintelligence.com/2020/10/vulnerability-spotlight-multiple.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+feedburner%2FTalos+%28Talos%E2%84%A2+Blog%29
Infected Technology	Synology Router Manager
Recommendation	Update the latest patch available
CVE_ID	CVE-2020-27648, CVE-2020-27650 CVE-2020-27652, CVE-2020-27656

5. Oracle WebLogic Server RCE Flaw Under Active Attack

Description	
Oracle WebLogic Server is a popular application server used in building and deploying enterprise Java EE applications. The console component of the WebLogic Server has a flaw, CVE-2020-14882. According to Oracle, the attack is "low" in complexity, requires no privileges and no user interaction and can be exploited by attackers with network access via HTTP.	
Source	https://www.helpnetsecurity.com/2020/10/29/cve-2020-14882/?web_view=true
Infected Technology	Oracle WebLogic server
CVE	CVE-2020-14882
Recommendation	Updates the patch available

6. Browser Bugs exploited to install backdoors on computers

Description	
Researchers have disclosed a new watering hole attack that exploits web browser vulnerabilities. Dubbed as Operation Earth Kitsune by Trend Micro, the campaign involves use of SLUB malware and two new backdoors to gain system information and gain additional control of compromised machine. The campaign is deploying multiple C&C servers and using exploits for multiple N-day bugs to leverage system access. The exploits used have been already patched by OEMs, however, are still in use by many end users and corporate houses.	
Source	https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations
Recommendation	Keep the security release up to date with the releases

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**