InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Millions of Computers Still Vulnerable to Bluekeep RDP Flaw
2. Firefox Releases Critical Patch Update to Stop Ongoing Zero-Day Attacks
3. O365 Phishing
4. Chrome Extensions caught hijacking users' search engine results
5. Vulnerability in TP-Link's Home Router
6. NVIDIA GeForce Experience OS Command Injection
7. TCP-based Remote Denial of Service Issues
8. Telegram hit by DDoS Attack

23/06/2019

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. Millions of Computers Still Vulnerable to Bluekeep RDP Flaw

Description	
Nearly 1 million Windows systems are still unpatched and have been found vulnerable to recently disclosed critical, wormable, remote code execution vulnerability in the Windows Remote Desktop Protocol (RDP)—two weeks after Microsoft releases the security patch. This vulnerability could allow an unauthenticated, remote attack to execute arbitrary code and take control of a targeted computer just by sending specially crafted requests to device's Remote Desktop Service (RDS) via the Remote Desktop Connection	
Source	**https://www.us-cert.gov/ncas/alerts/AA19-168A**
Infected Technology	**RDP**
Recommendation	**Update your device with latest patch**

2. Firefox Releases Critical Patch Update to Stop Ongoing Zero-Day Attacks

Description	
Mozilla earlier today released Firefox 67.0.3 and Firefox ESR 60.7.1 versions to patch critical zero-day vulnerability in the browsing software that hackers have been found exploiting in the wild. The vulnerability could allow attackers to remotely execute arbitrary code on machines running vulnerable Firefox versions and take full control of them.	
Source	**https://www.terabitweb.com/2019/06/20/tor-browser-8-5-2-html/**
Infected Technology	**Firefox**
Recommendation	**Update your firefox with latest patch**

3. O365 Phishing

Description	
Attackers are crafting and launching phishing campaigns targeting Office 365 users. The attackers attempt to steal a user's login credentials with the goal of taking over the accounts. If successful, attackers can often log into the compromised accounts, and perform a wide variety of malicious activity.	
Source	https://blogs.cisco.com/security/office-365-phishing-threat-of-the-month
Infected Technology	Office 365
Recommendation	Users should validate links before clicking.

4. Chrome extension caught hijacking users' search engine results

Description	
The extension named "YouTube Queue" allowed users to queue multiple YouTube videos in the order they wanted for later viewing. But under the hood, it also intercepted search engine queries, redirected the query through the Croowila URL, and then redirected users to a custom search engine named Information Vine, which listed the same Google search results but heavily infused with ads and affiliate links.	
Source	https://www.technadu.com/two-dragonblood-vulnerabilities-wpa3-wi-fi-standard/75933/
Infected Technology	Chrome Extensions
Recommendation	Do not download/install extensions without verifying

5. Vulnerability in TP-Link's Home Router

Description	
A vulnerability could give the attacker full access to the router's web management interface and thus manipulating its settings.	
Source	https://nvd.nist.gov/vuln/detail/CVE-2019-6971
Infected Technology	TP-Link Home Router
Recommendation	Check for firmware updates and patch if available

6. NVIDIA GeForce Experience OS Command Injection

Description	
This vulnerability allowed execution of arbitrary commands on a system with the NVIDIA GeForce Experience (GFE) prior to version 3.19 installed. The exploit can be achieved by convincing a victim to visit a crafted website and make a few key presses. This was possible due to command injection which was discovered in a local "Web Helper" server which GFE launches on startup.	
Source	https://rhinosecuritylabs.com/application-security/nvidia-rce-cve-2019-5678/
Infected Technology	GeForce Experience
Recommendation	The issue has been patched in a software update.

7. TCP-based Remote Denial of Service Issues

Description	
Three related flaws were found in the Linux Kernel's handling of TCP networking. The most severe vulnerability could allow a remote attacker to trigger a kernel panic in systems running the affected software and, as a result, impact the system's availability.	
Source	https://www.openwall.com/lists/oss-security/2019/06/17/5
Infected Technology	Linux Kernel
Recommendation	Update your linux system

8. Telegram Hit by DDoS Attack

Description	
Messaging service provider Telegram was hit by distributed denial- of service attack and users experienced connection issues. A DDoS attack floods your network, overwhelming your infrastructure – with up to Terabits per Second of garbage data – it doesn't matter how secure your service is. Nobody can access it. Sometimes it's used as an enabler for other cybercrimes. While services (including aspects of network security) are down, other malicious software may be infiltrated into your network devices resulting in massive data breaches, ransomware, theft of IP and more	
Source	https://securityboulevard.com/2019/06/telegram-hit-by-powerful- ddos-attack-blames-china/
Infected Technology	Telegram

For any queries/recommendations:

Contact us: whois@cryptogennepal.com