InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Remote Desktop Services with RCE Vulnerability
2. New Vulnerability in Microsoft's CTF Protocol
3. New HTTP/2 implementation flaw exposes websites to DoS Attacks
4. Over 40 drivers could let attackers install persistent backdoor on windows pcs
5. Kaspersky Security Flaw putting users at risks
6. Facebook sends audio data to third party contractors to transcribe

17/08/2019

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, Trip Advisor, 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. Remote Desktop Services with RCE Vulnerability

Description
Microsoft provides security update for windows' Remote desktop services that has a remote code execution vulnerability. Attackers can exploit the two wormable vulnerabilities by sending specially crafted requests to the Remote Desktop Service of targeted unpatched Windows systems via RDP. An attacker would be able to execute arbitrary code on the system which would enable the attacker to install programs, view, change, delete data or even create new accounts with full user rights.

Source	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
Infected Technology	Windows
Recommendation	Keep your systems up to date. Apply all available patches

2. New Vulnerability in Microsoft's CTF Protocol

Description
Security researcher Tavis Ormandy, with Google's Project Zero elite security team has discovered a vulnerability in Windows' CTF protocol that allows hackers or malware on user's computer to take over any app, high-privileged applications, or the entire OS. CTF is part of the Windows Text Services Framework that manages texts shown inside windows and windows application. The researcher discovered that the communications between CTF clients and the CTF servers aren't properly authenticated. An attacker can hijack another app's CTF session and then send commands to that app acting as a server.

Source	https://www.zdnet.com/article/vulnerability-in-microsoft-ctf-protocol-goes-back-to-windows-xp/
Infected Technology	Windows
Recommendation	Keep your systems up to date. Apply all available patches

3. New HTTP/2 implementation flaw exposes websites to DoS Attacks

Description
Today almost 40 percent of all the sites on the internet are running using HTTP/2 protocol. A total of eight vulnerabilities exist in HTTP/2 protocol due to resource exhaustion when handling malicious input, allowing a client to overload server's queue management code. The vulnerabilities can be exploited to launch Denial of Service (DoS) attacks against millions of online services and websites that are running on the web server, knocking them offline for everyone. According to CERT, affected vendors include NGINX, Apache, H20, Nghttp2, Microsoft (IIS), Cloudflare, Akamaim, Apple (SwiftNIO), Amazon, Facebook, Node.js and Envoy proxy.

Source	https://www.bleepingcomputer.com/news/security/new-http-2-flaws-expose-unpatched-web-servers-to-dos-attacks/
Infected Technology	HTTP/2

4. Over 40 drivers could let attackers install persistent backdoor on windows pcs

Description
A high-risk security vulnerability in more than 40 drivers have been discovered from at least 20 different vendors that could allow attackers to gain most privileged permission on that system. Since device drivers sit between the hardware and the operating system, in most cases have privileged access to the OS kernel, a security weakness in this component can lead to code execution at the kernel layer. This privilege escalation attack can move an attacker from user mode to kernel mode, allowing them to install a persistent backdoor in the system that a user would probably never realize.

Source	https://www.prodefence.org/over-40-drivers-could-let-hackers-install-persistent-backdoor-on-windows-pcs/
Infected Technology	System Drivers

5. Kaspersky Security Flaw putting users at risks

Description	
A German security journalist discovered a security flaw in Kaspersky Lab's Antivirus software. The researcher found that Kaspersky's antivirus software was injecting a Javascript script into web pages. The script is believed to be used to evaluate Google search result displayed in the user's browser. It is analyzing the user's web traffic and has information about all the websites users are visiting including inside secure corporate networks.	
Source	https://www.forbes.com/sites/jeanbaptiste/2019/08/16/warning-a-security-flaw-in-kaspersky-antivirus-lets-hackers-spy-users-online-millions-at-risk/
Infection Source	Kaspersky Antivirus

6. Facebook sends audio data to third party contractors to transcribe

Description	
Facebook reportedly collects audio data from users' voice chats and sends it to third-party contractors to transcribe. Facebook claimed that they only collected data from users who gave permission into having their chats transcribed. But sending the data to third party contractors have come into question as these are not mentioned in its data-use policies. Facebook collects and has contractors transcribe the audio data to check the accuracy of its automated speech-recognition systems.	
Source	https://www.bloomberg.com/news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio
Infection source	Facebook app

For any queries/recommendations:

Contact us: whois@cryptogennepal.com