InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Word Press Theme Plugin Opens 200,00 Sites to Hackers
2. Lenovo , HP , Dell Peripherals Face Unpatched Firmware Bugs
3. Two Critical Flaws were found in Adobe
4. SMS Attack Steals Bank Credentials
5. Critical Cisco Bug Opens Software

24/02/2020

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. **Word Press Theme Plugin Opens 200,00 Sites to Hackers**

Description	
A popular Word Press theme “ThemeGrill Demo Importer” plugin contains a severe but easy-to-exploit software vulnerability. When a ThemeGrill theme is installed and activated, the affected plugin executes some functions with administrative privileges without checking whether the user running the code is authenticated and is an admin. The flaw could eventually allow unauthenticated remote attackers to wipe the entire database of targeted websites to its default state, after which they will also be automatically logged in as an administrator, allowing them to take complete control over the sites.	
Source	https://threatpost.com/active-exploits-hit-vulnerable-wordpress-themegrill-plugin/152947/
Infected Technology	Word Press Websites
Recommendation	Update the latest patch

2. Lenovo , HP , Dell Peripherals Face Unpatched Firmware Bugs

Description	
A firmware vulnerabilities in Wi-Fi adapters, USB hubs, trackpads and cameras are putting millions of peripheral devices in danger of cyberattacks. A lack of proper code-signing verification and authentication for firmware updates opens the door to information disclosure, remote code execution, denial of service and more. TouchPad and TrackPoint firmware in Lenovo Laptops, HP Wide Vision FHD camera firmware in HP laptops and the Wi-Fi adapter on Dell XPS laptops were all found to lack secure firmware update mechanisms with proper code-signing. Firmware vulnerabilities could give adversaries full control over the compromised device,this could lead to implanted backdoors, network traffic sniffing, data exfiltration and more.	
Source	https://threatpost.com/lenovo-hp-dell-peripherals-unpatched-firmware/152936/
Infected Technology	Lenovo ,HP, Dell
Recommendation	Use proper signed firmware Apply latest firmware update

3. Two Critical Flaws Were Found in Adobe

Description
The two apps affected by the critical flaws are Adobe After Effects, a visual effects and motion graphics app used for post-production film making and video game production, and Adobe Media Encoder, an application to help with media processing requirements for audio and video.Both critical vulnerabilities exist due to out-of-bounds write memory corruption issues and can be exploited to execute arbitrary code on targeted systems by tricking victims into opening a specially crafted file using the affected software. Both vulnerabilities can be exploited by a remote, unauthenticated attacker via the internet, that if exploited, enable an attacker to execute remote code on targeted devices.

Source	https://thehackernews.com/2020/02/adobe-software-updates.html
Infected Industry	Adobe
Recommendation	Implement the latest update

4. SMS Attack Steals Bank Credentials

Description	
SMS attack “Smishing” a form of phishing that relies on text messages instead of email. Attackers are sending SMS messages to victims -pretending to be from their banks. Once they click on the links in the text messages, they are asked to hand over their banking credentials and download a file that infects their systems with the Emotet malware. When victims click on the link they see a customized phishing page that mimics the bank’s mobile banking page to persuade victims into entering their credentials as a first step, and then have them download a document file loaded with the malicious macros as a second step which let victims to lose their credential informations to the attackers.	
Source	https://threatpost.com/sms-attack-spreads-emotet-bank-credentials/153015/
Infected Industry	Mobile Banking App
Recommendation	Awareness related to Phishing attack

5.Critical Cisco Bug Opens Software Licensing Manager TO Remote Attack

Description
A critical flaw in the High Availability (HA) service of Cisco Smart Software Manager On-Prem Base has been found, which would open the door to remote attackers thanks to its use of a static, default password, even if the platform isn't directly connected to the internet. The hard-coded password is for a HA system account that is not under the control of the system administrator, so, anyone who discovered the password could log onto this account and then, from there, connect to the Cisco Smart Software Manager On-Prem Base.

Source	https://threatpost.com/critical-cisco-bug-software-licencing-remote-attack/153086/
Infected Technology	CISCO
Recommendation	update the latest patch available
CVE_ID	CVE-2020-3158

For any queries/recommendations:

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