InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Open SMPTD Vulnerability
2. Microsoft Azure Flaws Could Have Let Hackers Take Over Cloud Server
3. Wawa Breach
4. United Nations Reportedly hacked
5. Zoom Bug

03/02/2020

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. **Open SMPTD Vulnerability**

Description
New vulnerabilty disclosed in open SMTP email server that could control over BSD and other linux server by remote attacker.This vulnerability, the issue resides in the OpenSMTPD's sender address validation function, called smtp_mailaddr(), which can be exploited to execute arbitrary shell commands with elevated root privileges on a vulnerable server just by sending specially crafted SMTP messages to it.

Source	https://thehackernews.com/2020/01/openbsd-opensmtpd-hacking.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2154.qx0ao0e5ow.1cgc
Infected Technology	Open BSD version 6.6
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2020-7247

2. Microsoft Azure Flaws Could Have Let Hackers Take Over Cloud Server

Description
Two potentially dangerous vulnerabilities in Microsoft azure services were found, where an attacker can exploit both issues by creating a free user account with Azure cloud. The first vulnerability is a request spoofing issue that affected Azure Stack - a hybrid cloud computing software solution by microsoft, if exploited, this issue enables a remote hacker to unauthorizedly access screenshots and sensitive information on any virtual machine running in Azure infrastructure. The second vulnerability is a remote code execution flaw that affected the Azure App Service on Azure Stack, which could enable a hacker to take complete control over entire Azure Server and enterprises' business code.

Source	https://research.checkpoint.com/2020/remote-cloud-execution-critical-vulnerabilities-in-azure-cloud-infrastructure-part-i/
Infected Technology	Buisness running on Microsoft Azure
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2019-1234 CVE-2019-1372

3. Wawa Breach

Description	
It has been found that the Wawa store faced the data breach as Hackers had exposed payment card details of more than 30 million wawa breach victims on sale at dark market. The payment card detail includes card numbers, expiration dates and cardholder names. A data breach happened as Hackers had installed malware in the wawa's point-of sale server which stole payment detail of its customers form potentially all wawa locations.	
Source	https://thehackernews.com/2020/01/wawa-credit-card-breach.html
Infected Industry	Wawa
Recommendation	Please change credential or other details related to data breach

4. United Nation Reportedly Hacked

Description	
Reports have surfaced that the United Nations network had been hacked which the top officials tried to keep quiet. Reportedly several of the servers were compromised including UN's human rights office where sensitive data is collected. The leaked internal document which brought light to this case also says that the hackers exploited a flaw in Microsoft's SharePoint software to gain access to the network. However UN spokesperson has stated that no confidential data was compromised. The UN is a natural target for state-sponsored hacking, but news about major breaches is rare, as is firm attribution about who is responsible.	
Source	https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack
Infected Industry	United Nation network

5. Zoom Bug

Description	
Zoom hosts password-protected virtual meetings and conferences but also allows users to set up sessions for non-registered participants that can join active conversations without additional logins or passwords required. The only thing that such a person needs is a randomized 9, 10, or 11-digit meeting ID that is generated unique per each conversation. It such ID got leaked outside the intended group of people anyone that knows the meeting ID can join the meeting and obtain private, valuable or sensitive information unnoticed.one of the most commonly used conference platforms that popularized video conferencing software, patched a security flaw that allowed hackers to access various private conference calls unnoticed.	
Source	https://xiarch.com/blog/2020/01/30/zoom-bug-could-have-let-uninvited-people-join-private-meetings/
Infected Technology	Zoom Video Conference App
Recommendation	Update the latest patch released.

For any queries/recommendations:

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