InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Microsoft Support Record Exposed
2. Citrix Releases Final Patch as Ransomware Attacks Ramp Up
3. Vulnerabilities in Safari's Intelligent Tracking Protection
4. Cisco Warns of Critical Network Security Tool Flaw
5. Indonesia Credit Card Hackers For Magecart Attack

27/01/2020

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. Microsoft Support Record Exposed

Description
A data breach of 250 million Microsoft users has been brought to light. The researchers found that 250 million Customer Service and Support records were exposed on the web.Microsoft has since acknowledged the data breach saying it was due to "misconfiguration of an internal customer support database", which the company uses for tracking support cases. This includes logs of conversations between Microsoft support agents and customers of 14 years.

Source	https://www.cisomag.com/250-million-customer-records-exposed-due-to-misconfiguration-microsoft/
Infected Technology	Microsoft

2. Citrix Release Final Patch as Ransomware Attacks Ramp Up

Description
An unknown threat actor is actively scanning for and patching Citrix ADC servers exploitation attempts, while also deploying a new malware family dubbed NOTROBIN that drops a backdoor designed to maintain access to the compromised machines.Citrix released the final permanent fix for the actively exploited CVE-2019-19781 vulnerability. needed to secure all vulnerable Citrix Application Delivery Controller (ADC), Citrix Gateway, and Citrix SD-WAN WANOP appliances.

Source	https://www.forbes.com/sites/daveywinder/2020/01/25/critical-security-warning-as-shitrix-hackers-ramp-up-critical-citrix-vulnerability-cve201919781-attacks/#6668d47b29aa
Infected Industry	Citrix Application Delivery Controller Citrix Gateway Citrix SD-WAN WANOP
Recommendation	Update the Patch Available

3. Vulnerabilities in Safari's Intelligent Tracking Protection

Description	
Google researchers have exposed details of multiple security flaws in its rival Apple's Safari web browser that allowed users' browsing behaviour to be tracked, despite the fact that the affected tool was specifically designed to protect their privacy. The flaws, which were ironically found in an anti-tracking feature known as Intelligent Tracking Prevention.	
Source	https://threatpost.com/google-flaws-in-apples-private-browsing-technology-allow-for-third-party-tracking/152128/
Infected Technology	Safari
Recommendation	Update the latest Patch available

4. Critical Network Security Tool Flaw Cisco

Description
A Critical vulnerability was found in the web-based management interface of Cisco Firepower Management Center (FMC), which is its platform form managing Cisco network security solutions like Firewalls. The vulnerability occurred due to improper handling of Lightweight Directory Access Protocol(LADP) authentication responses from an external authentication server. The flaw could allow an unauthenticated, remote attacker to gain administrative privileges on impacted devices. An attacker could exploit this vulnerability by sending crafted HTTP requests to a vulnerable device.they could bypass authentication and gain administrative access to web-based management interface of the affected device.

Source	https://threatpost.com/cisco-critical-network-security-tool-flaw/152131/
Infected Technology	Cisco Fire Power Management Center (FMC)
CVE Details	CVE-2019-16028
Recommendation	Update the latest Patch released.

5. Indonesian Credit Card Hackers Targeting E-commerce Websites

Description	
An Indonesian hackers were found to be hacking hundreds of international e-commerce websites and stealing payment card details of their online shoppers. These hackers were found exploiting unpatched vulnerabilities in e-commerce websites powered by Magento and WordPress content management platforms. On those compromised websites, hackers then secretly implant digital credit card skimming code or web skimming code to intercept users input in real-time and steal their payment card number ,names, addresses and login details as well. These stolen information were used to buy electronic goods and other luxury items, and then also attempted to resell some of them at a relatively low price through local e-commerce website in Indonesia.	
Source	https://thehackernews.com/2020/01/indonesian-magecart-hackers.html
Infected Technology	E-commerce Websites
Recommendation	Update the latest Patch released.

For any queries/recommendations:

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