InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Microsoft IE Browse Zero-Day That's Under Active Attacks
2. Microsoft Patches Security Flaw
3. Critical Cisco Flaws
4. Honda Exposes 976 Million Records
5. Adobe Patch Released

20/01/2019

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. **Microsoft IE Browser Zero-Day That's Under Attacks**

Description	
Internet Explorer browser suffer an active Zero-day vulnerability that attackers are actively exploiting in the wild. The vulnerability is rated as moderate can allow a remote attacker to execute arbitrary code on targeted computers and take full control over them just by convincing victims into opening a maliciously crafted web page on the vulnerable Microsoft browser. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code and could gain the same user rights as the current user. In the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could gain the same administrative rights and could then install programs, view, change or delete data or create new accounts with full user rights.	
Source	https://thehackernews.com/2020/01/internet-explorer-zero-day-attack.html
Infected Technology	Microsoft (IE Browser)
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2020-0674

2. **Microsoft Patch Security Flaw**

Description	
Microsoft is patching a serious flaw in various versions of Windows today after the National Security Agency (NSA) discovered and reported a security vulnerability in Microsoft's handling of certificate and cryptographic messaging functions in Windows. The Flaw, which hasn't been marked critical by Microsoft, could allow attackers to spoof the digital signature tied to pieces of software, allowing unsigned and malicious code to masquerade as legitimate software and other critical flaws in Windows which affect RD gateway ,that can be exploited by unauthenticated attackers to execute malicious code on targeted systems just by sending a specially crafted request via RDP.	
Source	https://thehackernews.com/2020/01/warning-quickly-patch-new-critical.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2145.qx0a00e50w.1c8i
Infected Technology	Microsoft
Recommendation	Update your device the latest patch released
CVE_ID	CVE-2020-0601 (Windows CryptoAPI Spoofing Vulnerability) CVE-2020-0609, CVE-2020-0610 (Windows RDP Flaw)

3. Cisco Critical Flaws

Description	
Three critical vulnerabilities were identified in Cisco Center Network Manager (DCNM) tool that is used for managing network platform and switches. These three vulnerabilities were found in Cisco data centers that run Cisco's NX-OS - the network operating system used by Nexus-series Ethernet switches and MDS-series Fiber Channel storage area network switches. These flaws could allow an unauthenticated remote attacker to bypass endpoint authentication and execute arbitrary actions with administrative privileges on targeted devices. Two of the flaws are authentication bypass vulnerabilities in REST API and SOAP API endpoints for CIsco DCNM. And the third bug allow authentication bypass vulnerability that exist in web-based management interface of DCNM.	
Source	https://threatpost.com/cisco-dcnm-flaw-exploit/151949/
Infected Industry	Cisco
Recommendation	Patch to the latest update
CVE_ID	CVE-2019-15975, CVE-2019-15976, CVE-2019-15977

4. Honda Exposes 976 Million Records

Description	
Security Researcher discovered an unprotected Elasticsearch cluster which contained 976 million records belonging to "Honda North America". The database was left online without setting a password, so anyone with a web browser could potentially locate and access it. The researcher notified Honda's security team in Japan, who took it down on December 13, 2019, so the data has remained exposed for at least nine days. Out of the 976 million records that were contained in the unprotected database, an estimated 1 million corresponds to Honda vehicle owners' information.	
Source	https://www.securitynewspaper.com/2019/12/20/honda-is-hacked-personal-details-of-more-than-976-million-customers-leaked/
Infected Technology	Honda
Recommendation	Preventing misconfigurations would significantly reduce incidents of database information exposure in any company.

5. Adobe Patch Update

Description	
Adobe releases its first 2020 patch Tuesday software updates that address several vulnerabilities in Illustrator and Experience Manager products. *"Adobe has published security bulletins for Adobe Experience Manager (APSB20-01) and Adobe Illustrator (APSB20-03). Adobe recommends users update their product installations to the latest versions using the instructions referenced in the bulletin. The security updates for Illustrator CC 2019 for Windows addresses five critical memory corruption issues that can lead to arbitrary code execution in the context of the targeted user*. For Adobe Experience Manager (AEM) that addresses four issues rated important are Reflected Cross-Site Scripting cross-site scripting (XSS) and ated moderate has been described as a user interface injection issue and can lead to the disclosure of sensitive information.	
Source	https://www.zdnet.com/article/adobes-first-2020-security-patch-update-fixes-code-execution-vulnerabilities/
Infected Technology	Adobe
Recommendation	Update the latest patch released.

For any queries/recommendations:

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