June 22, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Vulnerability in Netgear Routers
- Adobe patches critical flaws in out of band updates
- Google removes 106 Malicious Chrome Extensions
- Ripple20 impacts millions of connected devices
- Oracle E-business Suits Flaw lets hackers control business operations
- Cisco Webex , Router Bug Allows Code Execution

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. Vulnerability in Netgear Routers

Description	
A new vulnerability was discovered in firmware for Netgear routers that put 76 device models at risk for full takeover. Reports by researchers say that the flaw is because of a memory safety issue present in the firmware's httpd web server. It allows attackers to bypass authentication on affected installations of Netgear routers. the problem is said to exist because of lack of support for a feature called stack canaries. Stack canaries are used to detect a stack buffer overflow before an execution of malicious code. Therefore, attacks can eventually lead to a stack-buffer overflow. Attackers can exploit recv function or use an CSRF attack to achieve this.	
Source	https://threatpost.com/netgear-zero-day-takeover-routers/156744/
Infected Technology	Netgear Routers
Recommendation	Restrict interaction with the service to trusted machines

2. Adobe patches critical flaws in out of band updates

Description	
Adobe patched critical vulnerabilities in Adobe After Effects, Illustrator, Premiere Pro, Premiere Rush and Audition. The vulnerabilities if exploited, allows an attacker to execute arbitrary code. Adobe After Effects' flaws include out-of-bounds read/write vulnerabilities and heap overflow flaws. Adobe Illustrator's flaws include buffer error and memory corruption bugs. Out-of-bounds read and out-of-bounds write vulnerabilities were also patched in Adobe Premiere Pro and Premiere Rush. Adobe's audio app Audition and Adobe Campaign Classic also had severe vulnerabilities which were patched in its latest updates.	
Source	https://threatpost.com/adobe-patches-18-critical-flaws-in-out-of-band-update/156609/
Infected Technology	Adobe After Effects, Premiere Pro, Illustrator, Premiere Rush, Audition, Campaign Classic
CVEs	CVE-2020-9661, CVE-2020-9660, CVE-2020-9662, CVE-2020-9637, CVE-2020-9638, CVE-2020-9642, CVE-2020-9575, CVE-2020-9641, CVE-2020-9640, CVE-2020-9639, CVE-2020-9656, CVE-2020-9657, CVE-2020-9655, CVE-2020-9653, CVE-2020-9654, CVE-2020-9658, CVE-2020-9659, CVE-2020-9666
Recommendation	Update to the latest patches

3. Google removes 106 Malicious Chrome Extensions

Description	
Google removed 106 malicious chrome extensions from Chrome Web Store with reports that they were being used to steal sensitive user data. The extensions were not only used to steal data but also to create persistent footholds on corporate networks. These extensions were free and designed to notify users to various websites or to convert files. Over 100 networks were abused, giving threat actors a foothold on financial service firms, oil and gas companies, healthcare and pharmaceutical industries and government organizations.	
Source	https://threatpost.com/google-yanks-106-malicious-chrome-extensions/156731/
Infected Platform	Google Chrome
Recommendation	Do not use untrusted extensions.

4. Ripple20 impacts millions of connected devices

Description	
A series of 19 different vulnerabilities are affecting hundreds of millions of IOT and Industry-controlled devices. The issue is in a TCP/IP software library developed by Treck, used by various manufacturers, built to handle TCP/IP protocol to connect devices to network and Internet. The issue is identified in more than 10 different manufacturer and expected to be found in dozens more. The devices using Treck's code include printers to medical infusion pumps. The vulnerabilities include four critical out of which two have CVSS score of 10 out of 10, one with 9.1 and other with 9 out of 10. The 3 out of 4 critical vulnerabilities allow remote code execution by forwarding malicious packets to the affected devices while other result in critical information disclosure. Other vulnerabilities include effect ranging from Denial of Service to potential remote code execution with score ranging from 3.1 to 8.2. Treck has issued the patch for OEMs to implement.	
Source	https://threatpost.com/millions-connected-devices-ripple20-bugs/156599/
Infected Technology	TCP/IP Software Library
CVEs	CVE-2020-11896, CVE-2020-11897, CVE-2020-11901, CVE-2020-11898, CVE-2020-11900, CVE-2020-11902, CVE-2020-11904, CVE-2020-11899, CVE-2020-11903, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914, CVE-2020-11908
Recommendation	Implement the patch once released by OEMs

5. Oracle E-business Suits Flaw lets hackers control business operations

Description	
Oracle's E-Business Suite (EBS) were found to have two vulnerabilities, dubbed BigDebIT which were patched in a critical patch update by Oracle. An enterprise cybersecurity firm Onapsis revealed the technical details of the vulnerabilities which has been rated a CVSS score of 9.9. Oracle's E-Business Suite is an integrated group of applications designed to automate CRM, ERP, and SCM operations for organizations. The security flaws could be exploited by threat actors to target accounting tools such as General Ledger to steal sensitive information and perform financial fraud.	
Source	https://thehackernews.com/2020/06/oracle-e-business-suite.html
Infected Technology	Oracle EBS Server
Recommendation	Patch the critical Vulnerabilities

6. Cisco Webex , Router Bug Allows Code Execution

Description	
Cisco is warning of three high-severity flaws in its popular Webex web conferencing app, including one that could allow an unauthenticated attacker to remotely execute code on impacted systems. The flaw stems from an improper validation of cryptographic protections, on files that are downloaded by the application as part of a software update. An attacker could exploit this vulnerability by persuading a user to go to a website that returns files to the client that are similar to files that are returned from a valid Webex website. The client may fail to properly validate the cryptographic protections of the provided files before executing them as part of an update. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the user.	
Source	https://threatpost.com/cisco-webex-router-code-execution/156706/
Infected Technology	Webex Meeting Desktop App for Mac
Recommendation	Update the Desktop App version 39.5.11 or higher

For any queries/recommendations:

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