October 19, 2020

INFOSEC WEEKLY

#MADE4SECURITY

1. Critical SonicWall VPN Portal bug allows DoS, leading RCE
2. QRadar vulnerable to remote attacks including Remote Code Execution
3. New Linux kernel flaw leading to Remote Code Execution
4. Microsoft fixes 87 vulnerabilities on Patch Tuesday
5. Juniper patch various vulnerabilities with critical severity
6. Adobe fixes Magento flaw leading to Code execution
7. Adobe released a patch for critical code execution vulnerability

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. Critical SonicWall VPN Portal bug allows DoS, leading RCE

Description	
A critical vulnerability in SonicOS, operating system on SonicWall Network Security Appliance (NSA), allows remote attacker to cause denial of service. The flaw is a stack-based buffer overflow in SonicWall Network Security Appliance (NSA). The vulnerable service is HTTP/HTTPS service used for product management and SSL VPN remote access. The identified vulnerability can also be leveraged to cause remote code execution, allowing attacker to create a botnet through worm. Almost 8,00,000 devices connected online are found vulnerable to the vulnerability however there is no sign of active exploitation yet.	
Source	https://www.tripwire.com/state-of-security/vert/sonicwall-vpn-portal-critical-flaw-cve-2020-5135/
Infected Technology	SonicOS 6.5.4.6-79n and earlier SonicOS 6.5.1.11-4n and earlier SonicOS 6.0.5.3-930 and earlier SonicOSv 6.5.4.4-44v-21-794 and earlier SonicOS 7.0.0.0-1
CVE	CVE-2020-5135
Recommendation	Update to the newer version

2. QRadar vulnerable to remote attacks including Remote Code Execution

Description	
A java deserialization bug in IBM's enterprise security tool allows attacker to conduct various attacks including remote code execution. The vulnerability could be exploited by passing malicious code to Servlet component of QRadar Community Edition. However, the vulnerability requires low privilege access to exploit it. The exploitation can lead to disclosure of sensitive information, local privilege escalation and execution of arbitrary code. The vulnerability has been fixed in QRadar CE October release.	
Source	https://www.ibm.com/support/pages/node/6344079
Infected Technology	IBM QRadar SIEM 7.4.0 - 7.4.1 GA IBM QRadar SIEM 7.3.0 - 7.3.3 Patch 4
CVE	CVE-2020-4280
Recommendation	Update the fixes released by IBM

3. New Linux kernel flaw leading to Remote Code Execution

Description	
Google has released details of high-severity Bluetooth stack flaw in Linux kernel supporting BlueZ which allows unauthenticated user to execute arbitrary code with kernel privilege. The vulnerability is found in Linux-based laptops and IoT devices. An attacker with vulnerable device's Bluetooth address can execute an arbitrary code with kernel privileges or cause denial of service. The unpatched second vulnerability is an information disclosure affecting Linux kernel 3.6 and higher. The third flaw is a heap-based buffer overflow impacting Linux kernel 4.19 and higher lead to arbitrary code execution or cause denial of service.	
Source	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html
Infected Technology	FortiGate VPN
CVE	CVE-2020-12351, CVE-2020-12352, CVE-2020-24490
Recommendation	Update the kernel fixes released.

4. Microsoft fixes 87 vulnerabilities on Patch Tuesday

Description	
Microsoft released patch for 87 vulnerabilities across its range of product. One of the critical vulnerabilities is a remote code execution in Windows TCP/IP stack that allows attacker to take over Windows systems by sending malicious ICMPv6 packets. Another critical vulnerability is also a RCE in Microsoft Outlook that fails to handle objects in the memory. The exploitation of the vulnerability requires user to open the specially crafted file in an email. The attack can also be executed by tricking user to visit a malicious website. Microsoft has also released advisories for other critical as well as Important patch releases in the reference link below which affects range of products including Server 2016 and 2019, SharePoint Enterprise Server 2016 and Windows 10.	
Source	https://portal.msrc.microsoft.com/en-us/security-guidance
Infected Technology	Microsoft Products
CVE	CVE-2020-16898, CVE-2020-16947
Recommendation	Update the patch released by Microsoft Apply the workaround for vulnerabilities

5. Juniper patch various vulnerabilities with critical severity

Description	
40 new vulnerabilities in JunOS which powers the company's firewalls and various third-party components. There seemed to be several vulnerabilities that have collectively been assigned a critical severity rating have been found in the Juniper Networks Mist Cloud UI. The bugs, related to Security Assertion Markup Language (SAML) authentication, allow a remote attacker to bypass SAML authentication. The company has released over a dozen advisories for high-severity vulnerabilities. Many of these weaknesses can be exploited for denial-of-service (DoS) attacks, but some could allow arbitrary code execution, including by sending specially crafted messages or via cross-site scripting (XSS).	
Source	https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES&cat=SIRT_1&actp=&sort=datemodified&dir=descending&max=1000&batch=15&rss=true&itData.offset=0
Infected Technology	Juniper JunOS
Recommendation	Apply the updates released by Juniper

6. Adobe fixes Magento flaw leading to Code execution

Description	
Arbitrary code execution and read or wire access to database vulnerabilities found in Magento. Magento is Adobe's commerce platform that is commonly targeted by attackers like the Magecart threat group. The issue stems from the application not validating full filenames when using an “allow list” method to check the file extensions. This could enable an attacker to bypass the validation and upload a malicious file. In order to exploit this flaw (CVE-2020-24407), attackers would not need pre-authentication. The other critical flaw is an SQL injection vulnerability. This is a type of web security flaw that allows an attacker to interfere with the queries that an application makes to its database. An attacker without authentication – but also with administrative privileges – could exploit this bug in order to gain arbitrary read or write access to a database.	
Source	https://helpx.adobe.com/security/products/magento/apsb20-59.html
Infected Technology	Magento
CVE	CVE-2020-24407
Recommendation	Apply the updates released

7. Adobe released a patch for critical code execution vulnerability

Description	
Adobe has released a patch for code execution vulnerability in its Flash Player. The attacker can use a specially crafted HTTP response to execute arbitrary code in the vulnerable system. There is no sigh of active exploitation however the vulnerability has been classified as critical. The vulnerability can also be exploited through embedded ActiveX control in Microsoft Office documents and applications using IE rendering engine.	
Source	https://helpx.adobe.com/security/products/flash-player/apsb20-58.html
Infected Technology	Adobe Flash Player Desktop Runtime Adobe Flash Player for Google Chrome Adobe Flash Player for Microsoft Edge and Internet Explorer 11
Recommendation	Apply the update released.

For any queries/recommendations:

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