August 17, 2020

INFOSEC WEEKELY

#MADE4SECURITY

- New vBulletin zero-Day Vulnerability
- Google Chrome Bug could let Hackers Bypass CSP protection
- Critical Flaws Affect Citrix Endpoint Management
- Flaws in Samsung phones exposes Android users to remote attacks
- Microsoft Reveals new innocent ways Windows users can get hacked
- SAP released security notes for August; critical vulnerabilities included
- RedCurl hackers steal corporate documents
- NSA disclosed new malware targeting Linux
- Emotet malware back with COVID-19 themed spam again

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. New vBulletin zero-Day Vulnerability

Description

VBulletin s a widely used proprietary Internet forum software package based on PHP and MySQL database server that powers over 100,000 websites on the Internet, including Fortune 500 and Alexa Top 1 million Companies websites and forums. A Security researcher has disclosed details and Proof-of-Concept exploit code for zero-day vulnerability in vBulletin. The zero-day is a bypass for a patch from previous vBulletin zero-day; namely CVE-2019-16759. The latest Zero-day vulnerability should be viewed as a severe issue because it is remotely exploitable and doesn't require authentication. It can easily be exploited using an exploit code of a single command that can result in RCE in the latest vBulletin software.

Source	https://blog.exploitee.rs/2020/exploiting-vbulletin-a-tale-of-patch-fail/
Infected Technology	VBulletin Forum
CVE_ID	• Disable PHP module in vBulletin Software • Upgrade their sites to run vBulletin 5.6.2 as soon as possible

2. Google Chrome Bug Could Let Hackers Bypass CSP Protection

Description

CSP is an extra layer of security that helps to detect and mitigate certain types of attacks, including cross-Site Scripting (XSS) and data injection attacks. With CSP rules, a website can mandate the victim's browser to perform certain client-side checks with an aim to block specific scripts that are designed to exploit the browser's trust of the content received from the server. Security researcher revealed details about a Zero-day flaw in chromium-based web browsers for Windows, MAC and Android that could allowed attackers to entirely bypass Content Security Policy (CSP) rules since Chrome 73.

Source	https://www.perimeterx.com/tech-blog/2020/csp-bypass-vuln-disclosure/
Infected Technology	Google Chrome
Recommendation	Update the Web Browser
CVE_ID	CVE-2020-6519

3. Critical Flaws Affect Citrix Endpoint Management

Description	
Citrix Endpoint management offers businesses mobile device management (MDM) and mobile application management (MAM) capabilities. It allows companies to control which apps their employees can install while ensuring updates and security setting are applied to keep business information protected. Citrix released patches for multiple new security vulnerabilities affecting its Citrix Endpoint management; called Xen Mobile. There are total of 5 vulnerabilities that affect on-premise instances of XenMobile servers used in enterprises to manage all apps, devices, or platforms from one central location. One of the critical flaws could allow an unauthenticated attacker to read arbitrary files outsides the web-server root directory, including configuration files and encryption keys for sensitive data.	
Source	https://support.citrix.com/article/CTX277457
Infected Technology	Citrix CEM
Recommendation	Patch their Systems to the latest versions of the software.
CVE_ID	CVE-2020-8208, CVE-2020-8209, CVE-2020-8210, CVE-2020-8211, CVE-2020-8212

4. Flaws in Samsung Phones Exposes Android Users to Remote Attacks

Description	
Samsung's Find My Phone service allows owner of Samsung devices to remotely locate or lock their smart phone or tablet, backup data stored on the devices to Samsung Cloud, wipe local data, and block access to Samsung Pay. There were four vulnerabilities in the app that could have been exploited by a malicious app installed on the targeted device, thus creating a man-in the-disk attack to hijack communication from the backend servers and snoop on victim. This flaws could have allowed remote attackers to track victims real-time location, monitor phone calls, and messages and even deleted data stored on phone.	
Source	https://char49.com/tech-reports/fmmx1-report.pdf
Infected Technology	Samsung smart phones
Recommendation	Tune Security policy to prevent unauthorized export

5. Microsoft Reveals new innocent ways Windows users can get hacked

Description	
Microsoft disclosed Software security updates for all Windows OS and other products. This month's update address total of 120 newly discovered Software vulnerabilities where 17 are critical. Windows computer can be hacked by playing video, listening audio, browsing website, editing an HTML page, reading PDF, receive an email message; where different apps of Microsoft have bug on it. Two of the security Flaws have reportedly been exploited by hackers in the wild. One of the zero-day vulnerability under active attack is a remote code execution bug that resides in the scripting engine's library jscript9.dll, which is used by default by all versions of Internet Explorer. The second zero-day vulnerability ; is a window incorrectly validates file signatures.	
Source	https://thehackernews.com/2020/08/microsoft-software-patches.html
Infected Technology	Microsoft Software and products
CVEs	CVE-2020-1380, CVE-2020-1464, CVE-2020-1472
Recommendation	Apply the latest security patch available.

6. SAP released security notes for August; critical vulnerabilities included

Description	
SAP has released a security patch with 16 advisories alerting critical and high severity in various products. The advisories include maximum severity RECON vulnerability used by unauthenticated attacker to access various folders in its directory structure. The security note also includes a critical XSS in Knowledge Management component of NetWeaver AS. Besides, high severity vulnerabilities like missing authentication check, missing authorization, Code injection, information disclosure and unrestricted file upload has been addressed in the release note.	
Source	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552603345
Infected Technology	Various SAP products and libraries used
CVEs	CVE-2020-6287, CVE-2020-6286, CVE-2020-6284, CVE-2020-6294, CVE-2020-6298, CVE-2020-6296, CVE-2020-6309, CVE-2020-6293, CVE-2020-6295, CVE-2020-6297, CVE-2020-6301, CVE-2020-6300, CVE-2020-6273, CVE-2020-6299, CVE-2020-6310
Recommendation	Apply the fix released by OEM

7. RedCurl hackers steal corporate documents

Description

RedCurl, a cyberespionage group which has been known for illicit activities from May 2018. The victims of groups are diversified in various industries span across different geographical location. The attackers deliver their payload via links of archives stored at multiple public cloud storage services. The attacker focuses to steal documentation and business emails from victims. The threat actor also uses open-source tool to steal credentials stored in memory and web browsers. On average, the attackers spend between two to six months allowing to shift through the infrastructure to gain required information.

Source	https://www.group-ib.com/resources/threat-research/red-curl.html
Threat vector	RedCurl
Recommendation	Make use of indicators of compromise (IOCs) released alongside the research to identify attack in early phase

8. NSA disclosed new malware targeting Linux

Description

National Security Agency (NSA) has issued a warning regarding operation from Russian Intelligence Directorate using a malware toolkit called Drovorub. The toolkit has various modules to ensure prevent detection, persistence and access to compromised machine. The rootkit communicates with C2 server which has read/write access, execute arbitrary commands with root privileges, communicate with network devices and survive reboots. NSA has released documents detailing the techniques to identify and mitigate the impact of malware.

Source	https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF
Infected Technology	Linux
Recommendation	Implement the mitigation technique in the reference material

9. Emotet malware back with COVID-19 themed spam again

Description	
Emotet malwares are back again with COVID-19 theme spam and is targeting end users rather than business houses. According to an independent research, Emotet is sending stolen email with malicious attachment, which when pressed enable content executes a PowerShell command to download multiple malware including Emotet from multiple sites. The malware leads to steal password, data and allow ransomware deployment.	
Source	https://www.bleepingcomputer.com/news/security/emotet-malware-strikes-us-businesses-with-covid-19-spam/
Infected Technology	Windows
Recommendation	• Do not open documents received from unknown source • Do not enable macros unless required

For any queries/recommendations:

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