September 14, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Linux Malware steals CDR from VoIP Softswitch Systems
- New Raccoon Attack Could Let Attackers Break SSL/TLS Encryption
- PIN Verification Bypass flaw affects Visa contactless payment
- BLURTooth Attacks
- Ransomware Hits US District Court in Louisiana
- Razer Gaffe Exposes Customer Data
- Attacks Targeting WordPress File manager Flaw
- Vulnerabilities in PAN-OS

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. Linux Malware steals CDR from VoIP Softswitch Systems

Description	
Cybersecurity researchers have discovered an entirely new kind of Linux malware dubbed 'CDR Thief' that targets voice over IP (VoIP) softswitches to steal phone metadata. The primary goal of the malware is to exfiltrate various private data from a compromised softswitch, including call details record (CDR). To steal this metadata, the malware queries internal MySQL databases used by softswitch. Thus, attackers demonstrate a good understanding of the internal architecture of the targeted platform. This malware had its malicious functionality encrypted to evade static analysis. The malware starts off by attempting to locate the SoftSwitch configuration files from a list of predetermined directories with goal of accessing the MySQL database credentials, which are then decrypted to query the database.	
Source	https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/
Infected Areas	VOIP platform

2. New Raccoon Attack Could Let Attackers Break SSL/TLS Encryption

Description	
Raccoon can allow a man-in-the-middle (MitM) attacker to crack encrypted communications that could contain sensitive information. However, the attack is only successful if the targeted server reuses public Diffie-Hellman (DH) keys in the TLS handshake (i.e. the server uses static or ephemeral cipher suites such as TLS-DH or TLS-DHE), and if the attacker can conduct precise timing measurements. The attacker needs circumstances for the Raccoon attack to work, needs to be close to the target server to perform high precision timing measurements and needs the victim connection to use DH(E) and the server to reuse ephemeral keys. And finally, the attacker needs to observe the original connection. The underlying vulnerability has existed for over 20 years, and it was fixed with the release of TLS 1.3.	
Source	https://raccoon-attack.com/
Infected Technology	F5, Microsoft, Mozilla, OpenSSL
Recommendation	• Update the latest patch available. • Recommend user to disable TLS_DHE

3. PIN Verification Bypass flaw affects Visa contactless payment

Description
A new flaw in Visa's EMV enabled cards was discovered by security researchers that allow cyber criminals to get funds and defraud cardholders and merchants illicitly. A PIN bypass attack that allows the criminals to get hold of a victim's stolen or lost credit card for making high-value purchases even without knowing the card's PIN, and also trick a point of sale (PoS) terminal into accepting an unauthentic offline card transaction. All contactless cards that use the Visa protocol, including Visa Credit, Visa Debit, Visa Electron, and V Pay cards, are affected by the security flaw. The researchers also stated that this could apply to EMV protocols implemented by Discover and UnionPay as well.

Source	https://emvrace.github.io/
Infected Technology	Visa Credit, Visa Debit, Visa Electron, V Pay cards, Discover and UnionPay
Recommendation	• Use Dynamic Data Authentication to secure high-value transaction • Required the use of online Cryptogram to all POS machine

4. BLURTooth Attacks

Description
Bluetooth SIG issued a statement informing users and vendors of a newly reported unpatched vulnerability that potentially affects hundreds of millions of devices worldwide. the flaw resides in the Cross-Transport Key Derivation (CTKD) of devices supporting both — Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth Low Energy (BLE) standard. Cross-Transport Key Derivation (CTKD) is a Bluetooth component responsible for negotiating the authenticate keys when pairing two Bluetooth devices together, also known as "dual-mode" devices. Dual-mode devices using CTKD to generate a Long Term Keys (LTK)or Link Key (LK) are able to overwrite the original LTK or LK in cases where that transport was enforcing a higher level of security.

Source	https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/blurtooth/
Infected Technology	Bluetooth
Recommendation	Restrict device to pair Bluetooth connection
CVE_ID	CVE-2020-15802

5. Ransomware Hits US District Court in Louisiana

Description	
Ransomware attack at US District Court in Louisiana exposed internal documents from the court and knocked its website offline. The infrastructure of US criminal court has been hit by ransomware, with court documents published online in what is thought to be the first Ransomware attack of its kind. Hacking group/ransomware strain Conti has claimed the attack on the Fourth District Court of Louisiana and published apparent proof of the attack on its dark web page this week. It appears to have published documents obtained from the court relating to defendant pleas, witnesses and jurors.	
Source	https://www.darkreading.com/attacks-breaches/ransomware-hits-us-district-court-in-louisiana/d/d-id/1338899?&web_view=true
Infected Areas	US District Court

6. Razer Gaffe Exposes Customer Data

Description	
The data of around 100,000 Razer customers has been exposed online following a misconfiguration faux pas. The lapse by global hardware manufacturing company and eSports and financial services provider. Customer data impacted by the cyber-slipup included full name, email, phone number, customer internal ID, order number, order details, and billing and shipping address. The data was part of a sizable log chunk stored on razer's Elasticsearch cluster that had been "misconfigured for public access and indeed by public search engines.	
Source	https://www.linkedin.com/pulse/thousands-razer-customers-order-shipping-details-web-diachenko/
Infected Areas	Razer gaffe
Recommendation	Beware of scams and phishing attacks

7. Attacks Targeting WordPress File manager Flaw

Description	
Threat actors are increasingly targeting a recently addressed vulnerability in the WordPress plugin File Manager. Researchers from WordPress security company Defiant observed a surge in the number of attacks targeting a recently addressed vulnerability in the WordPress plugin File Manager. hackers were actively exploiting a critical remote code execution vulnerability in the File Manager WordPress plugin that could be exploited by unauthenticated attackers to upload scripts and execute arbitrary code on WordPress sites running vulnerable versions of the plugin. The threat actors are already exploiting the flaw to upload malicious PHP files onto vulnerable sites.	
Source	https://www.wordfence.com/blog/2020/09/attackers-fight-for-control-of-sites-targeted-in-file-manager-vulnerability/
Infected Technology	WordPress version between 6.0- 6.8
Recommendation	Update the latest patch available

8. Vulnerabilities in PAN-OS

Description	
Attackers can use these vulnerabilities to gain access to sensitive data or develop the attack to gain access to the internal segments of the network of a company that uses vulnerable protection tools. PAN OS has multiple vulnerabilities has critical and high risk recently including Buffer overflow when captive portal or MFA is enabled, Reflected XSS, DOS, Command Injection and so on. Palo Alto Networks remediated vulnerabilities in Pan-OS.	
Source	https://www.helpnetsecurity.com/tag/palo-alto-networks/
Infected Technology	PAN-OS
CVE_ID	CVE-2020-2037, CVE-2020-2036, CVE-2020-2038, CVE-2020-2039
Recommendation	Update the latest available patch

For any queries/recommendations:

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