NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES

5th September 2019

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1: CYWARE (https://cyware.com/)

https://cyware.com/news/unsecured-server-exposes-419-million-records-of-phone-numbers-linked-to-facebook-accounts-d3653a06

Unsecured server exposes 419 million records of phone numbers linked to Facebook accounts. More than 419 million records linked to Facebook have been found in an unprotected server. This includes 133 million records belonging to users in the US, 18 million in the UK, and more than 50 million in Vietnam. Each record contained a user's unique Facebook ID and the phone number listed on the account. Some of the records also had the user's name, gender and geographical location.

https://cyware.com/news/attackers-demand-53-million-in-ransom-new-bedford-makes-counteroffer-for-400000-17d63177/

Attackers Demand $5.3 Million in Ransom, New Bedford Makes Counteroffer for $400,000. The city of New Bedford was hit by Ryuk ransomware on July 4, 2019. Following the attack, the city's IT network was affected and hackers had demanded a ransom of $5.3 million to decrypt the encrypted files. However, the city opted not to pay the ransom and reinstated the affected systems using backup files. It is said that the ransomware had encrypted files on 158 workstations.

System vulnerabilities

Source 1: CYWARE (https://cyware.com/)

https://cyware.com/news/android-smartphones-are-vulnerable-to-sms-phishing-attacks-88f8aef1

Android smartphones are vulnerable to SMS phishing attacks. A newly discovered security flaw in Android phones from Samsung, Huawei, LG, and Sony can leave users open to advanced phishing attacks. This could enable attackers to steal users' personal information. The flaw arises because the phones use over-the-air (OTA) provisioning. The attacker can make use of the OTA method to disguise their malicious SMS as an 'update network settings' text from the mobile network provider.

Source 2: Security Week (https://www.securityweek.com/)

https://www.securityweek.com/code-execution-flaws-found-ezautomation-plc-hmi-software

Code Execution Flaws Found in EZAutomation PLC, HMI Software. Security researchers have discovered vulnerabilities in two pieces of software made by EZAutomation, the U.S.-based industrial automation solutions provider. The potentially serious bugs - CVE-2019-13518 and CVE-2019-13522 - can be exploited for remote code execution. The vulnerabilities have been patched by EZAutomation in EZPLC Editor 1.9.0 and EZTouch Editor 2.2.0. The vendor has also advised users to only open project files from trusted sources.

Malware

Source 1: Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/security/ransomware-adopts-doppelpaymer-name-given-by-researchers/
Ransomware Adopts DoppelPaymer Name Given by Researchers. Threat actors from the INDRIK SPIDER cybercrime group have separated in order to create DopplePaymer. These are the same actors who created BitPaymer ransomware and research reveals that both share the same code, ransom note, and payment portal.

Source 2: CYWARE (https://cyware.com/)
https://cyware.com/news/new-glupteba-malware-variant-found-using-bitcoin-blockchain-to-update-c2-domains-5d71c7d3/
New Glupteba malware variant found using Bitcoin blockchain to update C2 domains. Security researchers have come across a new malvertising campaign that is distributing a new version of Glupteba malware. The malware was previously connected to a campaign called Operation Windigo carried out against Windows users. The new version includes an info-stealer component and an exploiter component targets Mikro Tik routers. The malware variant updates its C2 server using Bitcoin blockchain.

DDoS/Botnets

Source 1: CYWARE (https://cyware.com/)
https://cyware.com/news/android-trojan-called-joker-signs-users-up-for-premium-subscriptions-75d8ef31
Android Trojan called Joker signs users up for premium subscriptions. Joker is a new Android trojan that includes both malware dropper and spyware capabilities. The trojan was delivered via 24 Google Play Store apps that had more than 472,000 downloads. The additional malicious components include simulating user interaction on ad sites, harvesting victims' device info, contact list, and text messages.

Spam & Phishing

Source 1: CYWARE (https://cyware.com/)
https://cyware.com/news/scammers-mimic-sca-security-check-in-an-attempt-to-steal-users-bank-credentials-and-personal-data-d605a53a

Scammers mimic SCA security check in an attempt to steal users' bank credentials and personal data. Scammers are leveraging the new Strong Customer Authentication (SCA) regulation to trick users into sharing their personal details and banking credentials. They are mimicking the SCA-related messages and sending them through emails that appear to come from legitimate banks such as Santander, Royal Bank of Scotland (RBS) and HSBC. Each of these scam emails includes links to sites that are meant to capture personal details of users. The attacks are aimed at users in Europe. Users should be cautious about such emails and cross-check the links before providing their details.

Web security

Source 1: CYWARE (https://cyware.com/)

https://cyware.com/news/uc-health-fell-victim-to-phishing-attack-compromising-patient-information-243ad69b/

UC Health Fell Victim to Phishing Attack Compromising Patient Information. UC Health has disclosed a security breach that occurred due to unauthorized access between July 6 and July 12, 2019. The attackers behind the attack had targeted a limited number of employee email accounts. This had resulted in the compromise of patients’ names, birth dates, record numbers, and clinical information.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb19-245
Vulnerability Summary for the Week of August 26, 2019. Recorded by National Institute of Standards and Technology and National Vulnerability.

Source 2: Oracle Security Bulletins (http://www.oracle.com/technetwork/topics/security/alerts-086861.html)

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
Oracle Critical Patch Update Pre-Release Announcement - July 2019; advised action to run available security updates.

https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.html
Oracle Security Alert Advisory - CVE-2019-2729. Decentralization vulnerability in Oracle WebLogic Server exploitable without authentication requirements; advised action to run security updates.

https://www.oracle.com/technetwork/topics/security/bulletinjul2019-5600410.html
Oracle Solaris Third Party Bulletin - July 2019; advised action to apply necessary patches.

https://www.oracle.com/technetwork/topics/security/linuxbulletinjul2019-5600392.html
Oracle Linux Bulletin - July 2019; advised action to apply necessary Oracle Linux Bulletin fixes.

https://www.oracle.com/technetwork/topics/security/public-vuln-to-advisory-mapping-093627.html
Map of CVE to Advisory/Alert; advised action to apply the critical patch update for protection against known vulnerabilities.

https://www.oracle.com/technetwork/topics/security/ovmbulletinjul2019-5600406.html
Oracle VM Server for x86 Bulletin - July 2019; advised action to apply necessary Oracle VM Server for x86 Bulletin fixes.

Updates & Alerts

Source 1: Cisco Security Advisories & Alerts(http://tools.cisco.com/security/center/publicationListing.x)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-webex-teams

Cisco Webex Teams Logging Feature Command Execution Vulnerability. Due to improper restrictions on software logging features used by the application on Windows operating systems an unauthenticated, remote attacker could execute arbitrary commands on an affected system.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-ind

Cisco Industrial Network Director Configuration Data Information Disclosure Vulnerability. Due to improper access restrictions on the web-based management interface an unauthenticated, remote attacker could access sensitive information on an affected device.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-unified-ccx-ssrf

Cisco Unified Contact Center Express Request Processing Server-Side Request Forgery Vulnerability. Due to improper validation of user-supplied input on the affected system a remote attacker could bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-sma-info-dis

Cisco Content Security Management Appliance Information Disclosure Vulnerability. Due to incorrect permission controls role implementation an attacker could gain out-of-scope access to email.

Updates & Alerts

Source 2: Security Week (https://www.securityweek.com/)
https://www.securityweek.com/androids-september-2019-patches-fix-nearly-50-vulnerabilities
Android's September 2019 Patches Fix Nearly 50 Vulnerabilities. As a part of the September 2019 Patches, Google has released a new set of security patches that address nearly 50 vulnerabilities on the Android platform. The flaws impact Android versions 8.0, 8.1,9 and 10. 11 of these vulnerabilities are rated ‘High’ severity. Five of these impact Framework, while the remaining five are found in the System component of Android. In another incident, researchers have warned about a high-severity zero-day vulnerability in Google’s Android operating system. If exploited, the bugs could give a local attacker escalated privileges on a target’s device.

www.ke-cirt.go.ke