NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
6th September 2019

COMMUNICATIONS
AUTHORITY OF KENYA

Top Stories

Source 1: The Hacker News (https://thehackernews.com/)

https://thehackernews.com/2019/09/gps-tracking-device-for-kids.html

Flaws in Over Half a Million GPS Trackers Expose Children Location Data. 600,000 GPS trackers left exposed online with a default password of '123456'. Avast researchers found at least 600,000 GPS trackers manufactured by a Chinese vendor for keeping tabs on young children, elderly relatives, and pets containing a number of security vulnerabilities that were exposed online with a default password of "123456."

https://thehackernews.com/2019/09/youtube-kids-privacy-fine.html

Google Fined $170 Million For Violating Kids' Privacy On YouTube. Google has finally agreed to pay $170 million fine to settle allegations by the Federal Trade Commission and the New York attorney general that its YouTube service earned millions by illegally harvesting personal information from children without their parents' consent. The settlement requires Google to pay $136 million to the FTC and an additional $34 million fine to New York state for allegedly violating the Children's Online Privacy Protection Act (COPPA) Rule which requires child-directed websites and online services to explicitly obtain parental consent before collecting personal information from children under the age of 13 and then using it for targeted advertising.

https://thehackernews.com/2019/09/its-been-summer-of-ransomware-hold-ups.html

A Summer of Discontent: The Hottest Malware Hits. A recap of the most burning strains and trends in malware seen during the months of July and August 2019.

System vulnerabilities

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

https://www.bleepingcomputer.com/news/security/public-bluekeep-exploit-module-released-by-metasploit/

Public BlueKeep Exploit Module Released by MetaSploit. BlueKeep is a wormable Remote Code Execution (RCE) security flaw discovered in the Windows Remote Desktop Protocol (RDP) service which enables unauthenticated attackers to run arbitrary code remotely, to launch denial of service attacks, and, in some cases, to take full control of unpatched systems. A public exploit module for the BlueKeep Windows vulnerability has been added today to the open-source Metasploit penetration testing framework, developed by Rapid7 in collaboration with the open-source community.

Source 2: Security Affairs (https://securityaffairs.co/)

https://securityaffairs.co/wordpress/90893/hacking/exim-mail-server-flaw.html

CVE-2019-15846 Exim mail server flaw allows Remote Code Execution. A security flaw in Exim mail servers could be exploited by local or remote attackers to execute arbitrary code with root privileges.

Source 3: The Hacker News (https://thehackernews.com/)

https://thehackernews.com/2019/09/php-programming-language.html

Multiple Code Execution Flaws Found In PHP Programming Language. Hypertext Pre-processor (PHP) is the most popular server-side web programming language that powers over 78 percent of the Internet today. Maintainers at the PHP programming language have released new versions that address multiple flaws, including some code execution issues.

Malware

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

https://www.bleepingcomputer.com/news/security/gootkit-malware-bypasses-windows-defender-by-setting-path-exclusions/

GootKit Malware Bypasses Windows Defender by Setting Path Exclusions. GootKit is a banking Trojan, which uses a UAC bypass and WMIC commands to exclude the malware executable from being scanned by Windows Defender Antivirus. It attempts to steal the online banking credentials of infected users through video capture and redirects to fake banking sites under the attacker's control, it is a Node JS application packaged into an executable.

https://www.bleepingcomputer.com/news/security/lilocked-ransomware-actively-targeting-servers-and-web-sites/

Lilocked Ransomware Actively Targeting Servers and Web Sites. The ransomware is targeting servers and encrypting the data located on them. All of the known infected servers are web sites, which is causing the encrypted files to show up in Google search results. With a report that the attacker gained access to their web server using an Exim exploit. When a machine is infected, the ransomware will encrypt a file and then append the .lilocked extension to the file name.

DDoS/Botnets

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

https://cyware.com/news/fakespy-operators-target-japanese-users-with-new-funkybot-malware-ba2f035e/

FakeSpy operators target Japanese users with new FunkyBot malware. FunkyBot harvests a victim's list of contacts to ease its propagation process. In its last stage, the malware alters the device settings to make itself the default SMS handler application. It then uses this to upload to the C2 all the received messages. This functionality can be very dangerous, considering that most banks currently use two-factor authentication through SMS," Durando noted.

Spam & Phishing

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

https://cyware.com/news/hackers-leverage-salesforce-account-to-send-fake-invoices-in-new-phishing-attack-31bd10ae

Hackers leverage Salesforce account to send fake invoices in new phishing attack. The scam entails compromise of the company's Salesforce account to utilize Email Studio and send fake invoices to customers' emails. These fake invoices replicated the patterns of legitimate invoices and included several layers of Office 365 which made it difficult to be detected by email gateways.

Spam & Phishing

Source 2: Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/security/over-37-million-lost-by-toyota-boshoku-subsidiary-in-bec-scam/

Over $37 Million Lost by Toyota Boshoku Subsidiary in BEC Scam. Toyota Boshoku Corporation, a car components manufacturer member of the Toyota Group, announced today that one of its European subsidiaries lost more than $37 million following a business email compromise (BEC) attack. BEC scam refers to operations operated by scammers who attempt to deceive one or more employees of targeted organizations into wiring them money to bank accounts swapped with attacker-controlled ones.

Web security

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

https://cyware.com/news/unprotected-elasticsearch-database-belonging-to-dk-lok-exposes-private-and-confidential-emails-919c6856/

Unprotected Elasticsearch database belonging to DK-Lok exposes private and confidential emails. Researchers uncovered the leaky database during vpnMentor’s web mapping project, in which port scanning was used to find unprotected online systems. The open database was uncovered by the researchers through a vulnerability in a peripheral system linked to DK-Lok’s email hosting service, which has left its entire email database unsecured.

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 a 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 a 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 role permission controls implementation a remote attacker could gain out-of-scope access to email.

Updates & Alerts

Source 2: Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/microsoft/windows-10-insider-build-18975-released-with-movable-cortana-and-bug-fixes/

Windows 10 Insider Build 18975 Released With Movable Cortana and Bug Fixes. Microsoft has released Windows 10 Insider Preview Build 18975 (20H1) to Insiders in the Fast ring, which allows you to rename virtual desktops and the initial rollout of a new feature that allows you to resize and move Cortana.

www.ke-cirt.go.ke