NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
17th June 2020

COMMUNICATIONS AUTHORITY OF KENYA

Summary Headlines	Impact Metric Against Count of Events			
	Critical	High	Medium	Informative
Regional Highlights	0	0	0	2
Top Stories	0	3	0	0
System Vulnerabilities	0	1	1	0
Malware	0	1	2	0
DDoS/Botnets	0	1	0	0
Spam & Phishing	0	1	1	0
Web Security	0	1	0	
Updates & Alerts	2	0	1	0

COMMUNICATIONS AUTHORITY OF KENYA

Regional Highlights

Source 1 : The Standard (https://www.standardmedia.co.ke/)
https://www.standardmedia.co.ke/article/2001375522/two-charged-with-intercepting-security-cctv-footage-of-uhuru-entourage

Impact value: Informative

Two charged with intercepting security CCTV footage of Uhuru entourage on Kenyatta Avenue. Two Stanley Hotel employees were earlier today arraigned in a Nairobi court for allegedly leaking CCTV footage that captured President Uhuru Kenyatta and his entourage in the Nairobi Central Business District on June 2, 2019. Patrick Rading Ambogo and Janet Magoma Ayonga were charged with the offence of unauthorized interception of computer data contrary to section 17(1) of the Computer Misuse and Cyber Crime Act.

Source 2 : Techweez (https://techweez.com/)
https://techweez.com/2020/06/11/multichoice-bites-the-bullet-with-new-decoder-that-will-ship-with-netflix/

Impact value: Informative

Nairobi Courts Will Exclusively File Cases Electronically From Next Month. The Judiciary announced on 16 June a huge change in their workflow specifically for Nairobi courts. “It is hereby notified for public information that with effect from July 1 2020, the filing of cases in all the courts in Nairobi will be done exclusively through the Electronic Filing system, herein after referred to as e-filing,’ the Judiciary said in a communique on Twitter.

Top Stories

Source 1 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/wiggle-investigates-cyberattack/?&web_view=true
Impact value: High
Wiggle Investigates Cyber-Attack. Online sports retailer Wiggle is investigating a suspected cyber-attack after receiving a series of complaints from customers. Concerns were raised after customers received emails confirming orders for items from Wiggle that they had not placed. The suspicious orders were set to be delivered to addresses that the confused customers did not recognize.

Source 2 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/cia-unit-crafts-hacking-tools-didnt-protect-itself?&web_view=true
Impact value: High
CIA Unit That Crafts Hacking Tools Didn't Protect Itself. A specialized CIA unit that developed hacking tools and cyber weapons didn't do enough to protect its own operations and wasn't prepared to respond when its secrets were exposed, according to an internal report prepared after the worst data loss in the intelligence agency's history.

Source 3 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/north-koreas-state-hackers-caught-engaging-in-bec-scams/?&web_view=true
Impact value: High
'North Korea's state hackers caught engaging in BEC scams. At the ESET Virtual World security conference on Tuesday, security researchers from Slovak antivirus maker ESET have disclosed a new operation orchestrated by the regime's infamous state-sponsored hacker crews. Codenamed "Operation In(ter)ception," this campaign targeted victims for both cyber-espionage and financial theft.

System vulnerabilities

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

https://www.bleepingcomputer.com/news/security/plex-fixes-media-server-bugs-allowing-full-system-takeover/

Impact value: High

Plex fixes Media Server bugs allowing full system takeover. Plex has patched and mitigated three vulnerabilities affecting Plex Media Server for Windows that could enable attackers to take full control of the underlying system when chained together. Plex Media Server is a desktop app and the backend server for the Plex media streaming service, designed for streaming movies, TV shows, music, and photo collections to over the Internet and on local area networks. The three vulnerabilities tracked CVE-2020-5740, CVE-2020-5741, and CVE-2020-5742 were found by Tenable security researcher Chris Lyne and reported to Plex on May 31st.

https://www.bleepingcomputer.com/news/security/coinminer-exploits-apple-apsdaemon-vulnerability-to-evade-detection/

Impact value: Medium

CoinMiner exploits Apple APSDaemon vulnerability to evade detection. Malware distributors are abusing a DLL hijacking vulnerability in Apple's Push Notification service Windows executable to install coin miners on users attempting to download copyrighted software. A common method of generating revenue on warez and crack sites, adult sites, video sharing sites, and file-sharing sites is to open low-quality web pages when a visitor attempts to view or download content. These web pages redirect users through a series of sites that eventually push fake software updates, unwanted browser extension, fake giveaways, and malware.

Malware

Source 1 : Gdata (https://www.gdatasoftware.com/)
https://www.gdatasoftware.com/blog/strrat-crimson
Impact value: Medium
Amnesty Sounds Alarm Over Gulf, Norway Virus Apps. Amnesty International warned Tuesday that contact-tracing technology developed to contain the novel coronavirus threatens users' privacy, highlighting Bahraini, Kuwaiti and Norwegian apps as "among the most dangerous". Amnesty reported that the tools were frequently uploading GPS coordinates to central servers, meaning users' whereabouts could be tracked in real time.

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/linkedin-job-offers-targeted-aerospace-military-firms-with-malware/156614/
Impact value: Medium
LinkedIn 'Job Offers' Targeted Aerospace, Military Firms With Malware. Attackers are impersonating human resource employees from Collins Aerospace and General Dynamics in a spear-phishing campaign leveraging LinkedIn's messaging service. Targets are sent phony job offers that include malicious documents designed to fetch data-exfiltrating malware.

Source 2 : ZDnet (https://www.zdnet.com/)
https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/?web_view=true
Impact value: High
Citizen Lab and Amnesty International Uncover Spyware Operation Against Indian Human Rights Defenders. The targeting in this campaign occurred between January and October 2019. Targets were sent emails disguised as important communications, such as official summonses, bearing links to malicious software disguised as important documents. If opened, targets' computers would have been infected with NetWire, a piece of commodity malware.

Botnets/DDoS

Source 1 : Dark Reading (https://www.darkreading.com/)
https://www.darkreading.com/attacks-breaches/hosting-provider-hit-with-largest-ever-ddos-attack/d/d-id/1338107?&web_view=true

Impact value: High

Hosting Provider Hit With Largest-Ever DDoS Attack. Attackers leveled a massive distributed denial-of-service attack against a specific website in early June, topping a bandwidth of 1.44 terabits-per-second and 385 million packets-per-second, the largest volumetric attack encountered by Internet infrastructure firm Akamai.

Spam & Phishing

Source 2 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/detect-alert-scam-ads/?&web_view=true

Impact value: Informative

New Fake Ad Alert System Launched to Fight Online Scams. A new system to detect and remove scam adverts from the internet has been launched in the UK. set up by the Advertising Standards Authority (ASA) and the Internet Advertising Bureau (IAB) with support from digital ad platforms and tech giants. This tool will allow people to report scam ads which appear in paid-for spaces online. The ASA will then circulate details of the ads, remove them and suspend the advertiser's account where possible.

Source 3 : Tripwire (https://www.tripwire.com/)
https://www.tripwire.com/state-of-security/security-data-protection/sextortionists-using-social-engineering-tactics-to-collect-victims-data/?web_view=true

Impact value: Medium

Sextortionists Using Social Engineering Tactics to Collect Victims' Data. Security researchers observed sextortionists leveraging social engineering techniques to steal their victims' personal information. SANS' Internet Storm Center (ISC) discovered that sextortionists had begun creating profiles for young women on dating websites. They used those profiles and the stated interest of finding "good times" to connect with new contacts on the platforms. spam

Web Security

Source 1 : The Register (https://www.theregister.com/)
https://www.theregister.com/2020/06/17/cloud_services_hacking/?&web_view=true
Impact value: Informative
Researchers find abuse of cloud platform by hackers and security researchers alike. In a recent research paper titled "Cloud as an Attack Platform" [PDF], five boffins from Texas Tech University – Moitrayee Chatterjee, Prerit Datta, Faranak Abri, Akbar Siami-Namin, and Keith Jones – describe a series of interviews they conducted with computer security pros attending the Black Hat and DEF CON conferences. Of the 75 security professionals and hackers they spoke with as a part of a larger examination of attacker psychology, more than 93 per cent admitted to abusing cloud services to create attack environments and launch attacks.

Source 2 : Cyber News (https://cybernews.com/)
https://cybernews.com/security/italian-sales-agents-personal-data-leaked-by-mlm-company/?web_view=true
Impact value: High
30,000+ Italian sales agents' personal data, IDs leaked by MLM company that distributes wellness products. Cyber News recently uncovered an unsecured Amazon Simple Storage Service (S3) bucket that contains more than 36,000 documents, including scans of national IDs, credit cards, and health insurance cards. The database also contains sales representative enrollment contracts that include personally identifiable information such as full names, addresses, tax identification numbers, and signatures of mostly Italian citizens.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb20-160
Vulnerability Summary for the Week of June 1, 2020. 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/security-alerts/cpujan2020.html
Oracle Critical Patch Update Advisory - January 2020; advised action to run available security updates.

https://www.oracle.com/security-alerts/alert-cve-2019-2729.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/security-alerts/bulletinoct2019.html
Oracle Solaris Third Party Bulletin - October 2019; advised action to apply necessary patches.

https://www.oracle.com/security-alerts/linuxbulletinoct2019.html
Oracle Linux Bulletin - October 2019; advised action to apply necessary Oracle Linux Bulletin fixes.

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

https://www.oracle.com/security-alerts/linuxbulletinoct2019.html
Oracle VM Server for x86 Bulletin - October 2019; advised action to apply necessary Oracle VM Server for x86 Bulletin fixes.

Updates & Alerts

Source 1 : Dark Reading (https://www.darkreading.com/)
https://www.darkreading.com/vulnerabilities---threats/microsoft-releases-update-for-dos-flaw-in-net-core-/d/d-id/1338089?&web_view=true
Impact value: Medium
Microsoft Releases Update for DoS Flaw in .NET Core. Last week Microsoft published a revision to CVE-2020-1108, a denial-of-service (DoS) vulnerability in the .NET Core and .NET Framework. To fully address the flaw, the company released updates for PowerShell Core 6.2 and PowerShell 7.0, according to an email advisory sent on June 11.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/vlc-media-player-3011-fixes-severe-remote-code-execution-flaw/
Impact value: Critical
VLC Media Player 3.0.11 fixes severe remote code execution flaw. VideoLan has released VLC Media Player 3.0.11, and it is now available for Windows, Mac, and Linux. In addition to bug fixes and improvements, this release also fixes a security vulnerability that could allow attackers to remotely execute commands or crash VLC on a vulnerable computer. This vulnerability is tracked as CVE-2020-13428 and is a "buffer overflow in VLC's H26X packetizer" that would allow attackers to execute commands under the same security level as the user if properly exploited.

https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-flaws-in-illustrator-after-effects-more/
Impact value: Critical
Adobe fixes critical flaws in Illustrator, After Effects, more. Adobe has released out-of-band security updates to address 18 critical flaws that could allow attackers to execute arbitrary code on systems running vulnerable versions of Adobe After Effects, Illustrator, Premiere Pro, Premiere Rush, and Audition on Windows and macOS devices.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke