NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
26th May 2020

COMMUNICATIONS AUTHORITY OF KENYA

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

COMMUNICATIONS AUTHORITY OF KENYA

Regional Highlights

Source : Techweez (https://techweez.com/)
https://techweez.com/2020/05/27/court-of-appeal-multichoice-locked-set-top-box/
Impact value: Informative
Court of Appeal Rejects Multichoice's Appeal on Sale of Locked Set-Top Boxes. Subscription television service providers will no longer lock out competitors from using their set-top boxes to broadcast content. Justice Mumbi Ngugi from the High Court directed that all set-top boxes be open and operable between networks. However, MultiChoice decided to move the case to the Court of Appeal. The company argued that Justice Ngugi ought to have restricted herself to the licensing of the signal distribution.

Top Stories

Source 1 : Yahoo (https://in.finance.yahoo.com/)

https://in.finance.yahoo.com/news/cyber-criminal-put-truecaller-records-134149107.html?&web_view=true

Impact value: High

Cyber criminal put Truecaller records of 47.5 million Indians on sale. A cyber criminal has put on sale records of 47.5 million Indians claimed to be sourced from online directory Truecaller for about Rs 75,000, according to online intelligence firm Cyble. 'Our researchers have identified a reputable seller, who is selling 47.5 million Indians Truecaller records for USD 1,000 (about Rs 75,000). The data is from 2019. We were also taken off by surprise with such a low price point,' Cyble said in a blog. The data on sale includes phone numbers, gender, city, mobile network, Facebook id etc.

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

https://www.bleepingcomputer.com/news/security/26-million-livejournal-accounts-being-shared-on-hacker-forums/

Impact value: High

26 million LiveJournal accounts being shared on hacker forums. A database containing over 26 million unique LiveJournal user accounts, including plain text passwords, is being shared for free on multiple hacker forums. For some time, rumors have been circulating that LiveJournal was breached in 2014 and account credentials for 33 million users were stolen. Since approximately May 8th, 2020, links to a data dump allegedly containing 33,717,787 unique accounts have been circulating on various hacker forums.

System vulnerabilities

Source 1 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/vulnerabilities-found-emerson-scada-product-made-oil-and-gas-industry
Impact value: Critical
Flawed SCADA product. Four vulnerabilities discovered in Emerson OpenEnterprise, a SCADA solution designed for the oil and gas industry, can allow attackers to take control of systems. The four flaws originate from heap-based buffer overflow, missing authentication, improper ownership management, and weak encryption issues. Two of them are critical flaws and are tracked as CVE-2020-6970 and CVE-2020-1064. These two flaws can allow attackers to remotely execute arbitrary code with elevated privileges on devices running OpenEnterprise.

Source 2 : Yahoo (https://in.finance.yahoo.com/)
https://finance.yahoo.com/news/android-bug-strandhogg-2-0-120052295.html?&web_view=true
Impact value: High
A new Android bug, Strandhogg 2.0, lets malware pose as real apps and steal user data. Security researchers have found a major vulnerability in almost every version of Android, which lets malware imitate legitimate apps to steal app passwords and other sensitive data. Strandhogg 2.0 works by tricking a victim into thinking they're entering their passwords on a legitimate app while instead interacting with a malicious overlay. Strandhogg 2.0 can also hijack other app permissions to siphon off sensitive user data, like contacts, photos, and track a victim's real-time location.

Malware

Source 1 : We Live Security (https://www.welivesecurity.com/)
https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/
Impact value: High
ComRAT v4. Turla threat actor group updated its ComRAT backdoor to exfiltrate antivirus logs from victim organizations. The new version, ComRAT v4, was recently used in a cyber espionage campaign targeted against three high-profile entities that included a national parliament in the Caucasus and two Ministries of Foreign Affairs in Eastern Europe. The malware receives commands through the Gmail web interface.

Source 2 : Helpnet Security (https://www.helpnetsecurity.com/)
https://www.helpnetsecurity.com/2020/05/26/windows-malware-rdp-backdoor/
Impact value: High
New Sarwent malware variant opens RDP backdoor into Windows systems. Security researchers have uncovered a new variety of Sarwent malware that allows cybercrooks to gain access to Windows machines via the Remote Desktop Protocol (RDP) port. This new variant can also enable threat actors to create a new Windows user account on an infected system.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/hacking-group-builds-new-ketrum-malware-from-recycled-backdoors/
Impact value: Informative
Hacking group builds new Ketrum malware from recycled backdoors. The Ke3chang hacking group historically believed to be operating out of China has developed new malware dubbed Ketrum by merging features and source code from their older Ketrican and Okrum backdoors. Ke3chang's operations target a wide range of military and oil industry entities, as well as government contractors and European diplomatic missions and organizations.

Botnets/DDoS

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/rangeamp-attacks-can-take-down-websites-and-cdn-servers/
Impact value: High
RangeAmp attack. A team of academics has found a new way to launch large-scale DoS attacks. Termed as RangeAmp, the technique exploits HTTP range requests to cause network congestion by amplifying the web traffic. So far, the team has discovered two variants of the attack - RangeAmp Small Byte Range (SBR) attack and RangeAmp Overlapping Byte Ranges (OBR) attack.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/qihoo-baidu-disrupt-malware-botnet-with-hundreds-of-thousands-of-victims/
Impact value: Informative
Qihoo & Baidu disrupt malware botnet with hundreds of thousands of victims. For the past three years, the DoubleGuns trojan has emerged to take the crown as one of China's largest malware botnets. DoubleGuns is a malware trojan that targets Windows devices. Qihoo says that since May 14, they've been working with Baidu in a joint operation to take down some of the botnet's backend infrastructure, most of which has been using Baidu's Tieba image hosting service.

Spam & Phishing

Source 3 : CISO (https://ciso.economictimes.indiatimes.com/)
https://ciso.economictimes.indiatimes.com/news/facebook-introducing-in-app-notifications-feature-in-messenger-to-warn-about-potential-scammers/75990973
Impact value: Informative
Facebook introducing in-app notifications feature in Messenger to warn about potential scammers. According to Mashable, if you're talking to someone and they ask for money out of nowhere, Messenger will essentially tap you on the shoulder with these "safety notices" and pop up a "Steps you can take" alert, suggesting what you should do in order to avoid a potential scam or fraud. The feature goes live for both iOS and Android users.

Web Security

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/arbonne-mlm-data-breach-exposes-user-passwords-personal-info/
Impact value: High
Arbonne MLM data breach exposes user passwords, personal info. International multi-level marketing (MLM) firm Arbonne International exposed the personal information and credentials of thousands after its internal systems were breached by an unauthorized party last month. According to Arbonne's breach notification, 3,527 California residents were impacted in the incident, with the following types of personal information being exposed to unauthorized access: names, email and mailing addresses, order purchase histories, phone numbers, and Arbonne account passwords.

Source 2 : News18 (https://www.news18.com/)
https://www.news18.com/news/tech/hacker-selling-80000-users-data-stolen-from-cryptocurrency-wallets-2636021.html?&web_view=true
Impact value: High
Hacker Selling 80,000 Users' Data Stolen From Cryptocurrency Wallets. A hacker who was behind the cyber attack on Ethereum.org is now selling data tied to key cryptocurrency wallets like Keepkey, Trezor, Ledger and online investment platform Bnktothefuture. The hacker has three large databases with information pertaining to at least 80,000 customers. This includes the customer's email address, name, phone number, residential address and other data.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb20-118
Vulnerability Summary for the Week of April 20, 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 : Cisco (https://tools.cisco.com/)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-mds-ovrld-dos

Impact value: High

Cisco MDS 9000 Series Switches Denial of Service Vulnerability. The vulnerability is due to improper resource usage control. An attacker could exploit this vulnerability by sending traffic to the management interface (mgmt0) of an affected device at very high rates. An exploit could allow the attacker to cause unexpected behaviors such as high CPU usage, process crashes, or even full system reboots of an affected device.

Source 2 : ZDnet (https://www.zdnet.com/)

https://www.zdnet.com/article/samsung-develops-new-security-chip-for-smartphones/

Impact value: Informative

Samsung develops new security chip for smartphones. Samsung has launched a new secure element (SE) chip to protect private and sensitive data on mobile devices, the company said on Tuesday. The chip, dubbed S3FV9RR, will be offered as a standalone turnkey with security software, Samsung said. According to Samsung, the new chip provides protection for mobile devices such as smartphones and tablets when performing booting, isolated storage, mobile payment, among other applications.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke