NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES

10th 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	3	0	0
System Vulnerabilities	0	2	0	0
Malware	0	3	0	0
DDoS/Botnets	0	0	1	0
Spam & Phishing	0	0	2	0
Web Security	0	3	0	0
Updates & Alerts	0	1	0	2

Regional Highlights

Source : The Standard (https://www.standardmedia.co.ke/)
https://www.standardmedia.co.ke/business/article/2001370567/treasury-eyes-online-firms-to-grow-tax-revenues
Impact value: Informative

Treasury hits online trade with new levy as it aims to grow tax revenues. The government plans to impose a 1.5 per cent tax on products that are sold through online platforms as it seeks to grow tax revenues. In the Finance Bill 2020 tabled on Thursday in Parliament, the tax will be remitted by the eCommerce firms trading online.

“A tax to be known as the digital service tax shall be payable by a person whose income from the provision of services is derived from or accrues in Kenya through a digital market place,” reads the Finance Bill 2020.

Top Stories

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/hackers-sell-stolen-user-data-from-homechef-chatbooks-and-chronicle/
Impact value: High
HomeChef's stolen data on sale. Shiny Hunters group, which previously offered databases of Tokopedia, Unacademy, and Microsoft's GitHub repositories for sale, is now selling user records stolen from HomeChef, ChatBooks, and Chronicle.com. Altogether, the three databases contain 26 million accounts and are set at prices between $1,500 and $2,500.

https://www.bleepingcomputer.com/news/security/rail-vehicle-manufacturer-stadler-hit-by-cyberattack-blackmailed/
Impact value: High
Rail vehicle manufacturer Stadler hit by cyberattack, blackmailed. International rail vehicle construction company, Stadler, disclosed that it was the victim of a cyberattack which might have also allowed the attackers to steal company and employee data. The Swiss-based company has a workforce of roughly 11,000 employees based in 7 production locations, 5 component manufacturing sites, and 40 service locations around the world.

Source 2 : Security Affairs (https://securityaffairs.co/)
https://securityaffairs.co/wordpress/102916/hacking/ruhr-university-bochum-attack.html
Impact value: High
Ruhr University Bochum attacked. The Ruhr University Bochum (RUB) shut down its central IT infrastructure after falling victim to cyberattacks between May 6 and May 7, 2020. The university is currently investigating the incident to understand the extent of the attack.

System vulnerabilities

Source 1 : Trustwave (https://www.trustwave.com/)
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/vulnerabilities-in-schneider-electric-somachine-and-m221-plc/
Impact value: High
Stuxnet-type vulnerability. Researchers have uncovered another vulnerability in Schneider Electric software similar to the one exploited by the notorious Stuxnet malware. Tracked as CVE-2020-7489, the flaw has a score of 8.2 on the CVSS scale. It affects the Schneider SoMachine Basic v1.6 engineering software.

Source 2 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/search-company-algolia-hacked-recent-salt-vulnerabilities
Impact value: High
Search Company Algolia Hacked via Recent Salt Vulnerabilities. US startup Algolia has become the latest victim of a Salt vulnerability. Threat actors exploited a recently patched vulnerability, CVE-2020-11651, to install both a cryptocurrency miner and a backdoor on multiple Algolia servers.

Malware

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

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-can-now-encrypt-open-and-locked-files/

Impact value: High

Sodinokibi ransomware can now encrypt open and locked files. The Sodinokibi (REvil) ransomware has added a new feature that allows it to encrypt more of a victim's files, even those that are opened and locked by another process. When a file is locked, this also prevents ransomware applications from encrypting them without first shutting down the process that locked the file.

https://www.bleepingcomputer.com/news/security/new-aria-body-backdoor-gets-advanced-hackers-back-in-the-spy-game/

Impact value: High

New "Aria-body" backdoor gets advanced hackers back in the spy game. An advanced hacker group running cyber-espionage campaigns since at least 2010 has been operating stealthily over the past five years. They deliver a new backdoor called Aria-body and use victims’ infrastructure to carry attacks against other targets.

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

https://securityaffairs.co/wordpress/102858/cyber-crime/brazilian-trojan-banker-targets-portugal.html

Impact value: High

Brazilian trojan banker is targeting Portuguese users using browser overlay. Since the end of April 2020, a new trojan has been affecting Portuguese users from several bank organizations. The first stage of this malware is an MSI (Microsoft Installer) file that downloads the malware from a google-sites server and deploys it in the Windows startup folder. After that, the infected computer is restarted to make the trojan persistent.

Botnets/DDoS

Source 1 : Hack Read (https://www.hackread.com/)
https://www.hackread.com/ddos-for-hire-service-superiorstresser-operator-suspended-sentence/?web_view=true
Impact value: Medium
SuperiorStresser DDoS-For-Hire Service Offered as Low as £8 to Carry Out DDoS Attack. 20-year old Joseph Connolly from Banstead, Surrey has received a suspended sentence for selling cyber-attack service that could have caused permanent reputational and financial losses to businesses and individuals. The teen was charged with money laundering and cybercrime offenses to which he pleaded guilty while being prosecuted at a Guilford Crown Court.

Spam & Phishing

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/microsoft/microsoft-edge-is-getting-a-new-feature-to-reduce-web-spam/
Impact value: Informative
Microsoft Edge is getting a new feature to reduce web spam. Microsoft Edge is now giving users the ability to hide those pesky browser notification dialog boxes that are commonly used by web sites to push their content, or even spam, on visitors. While notification subscription dialogs are annoying from legitimate sites, they are even more annoying from the multitude of scam sites that abuse them.

https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-out-protection-against-office-365-email-storms/
Impact value: Informative
Microsoft rolls out protection against Office 365 email storms. Microsoft is rolling out protection against Office 365 Reply-All email storms, an issue impacting Exchange Online users who are members of large and improperly locked down mail distribution lists.

Web Security

Source 1 : Threat Post (https://threatpost.com/)
https://threatpost.com/hackers-breach-3-5-million-mobifriends-dating-app-credentials/155590/
Impact value: High
Hackers Breach 3.5 Million MobiFriends Dating App Credentials. The credentials of 3.5 million users of MobiFriends, a popular dating app, have surfaced on a prominent deep web hacking forum, according to researchers. Researchers say the leaked data include dates of birth, genders, website activity, mobile numbers, usernames, email addresses and MD5 hashed passwords.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/a-hacker-group-is-selling-more-than-73-million-user-records-on-the-dark-web/
Impact value: High
A hacker group is selling more than 73 million user records on the dark web. A hacking group has started to flood a dark web hacking marketplace with databases containing a combined total of 73.2 million user records over 11 different companies. For the past week, a hacking group known as Shiny Hunters has been busy selling a steady stream of user databases from alleged data breaches.

https://www.zdnet.com/article/digital-ocean-says-it-exposed-customer-data-after-it-left-an-internal-doc-online/
Impact value: High
Digital Ocean says it exposed customer data after it left an internal document online. Web hosting provider Digital Ocean is currently in the process of notifying some customers about a security lapse that exposed some of their account details. According to an email the company is currently sending out, the security leak occurred due to an internal Digital Ocean document that was mistakenly left accessible online. Digital Ocean says the document contained several types of user account details.

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 : Threat Post (https://threatpost.com/)
https://threatpost.com/cisco-fixes-high-severity-flaws-in-firepower-security-software-asa/155568/
Impact value: High
Cisco has fixed 12 high-severity flaws in its Adaptive Security Appliance software and Firepower Threat Defense software. Cisco has stomped out 12 high-severity vulnerabilities across several network security products. The flaws can be exploited by unauthenticated remote attackers to launch an array of attacks – from denial of service (DoS) to sniffing out sensitive data.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/new-google-authenticator-update-makes-it-worth-using-again/
Impact value: Informative
New Google Authenticator update makes it worth using again. Google has released the first update for Google Authenticator in years and it comes with the long-awaited feature of being able to move 2FA accounts between devices. Once an account is created on the authentication app, it will allow you to generate tokens that are only valid for a short period of time and need to be entered into a site before logging in.

https://www.bleepingcomputer.com/news/microsoft/windows-10-upgrade-bug-prevents-hdr-video-streaming/
Impact value: Informative
Windows 10 upgrade bug prevents HDR video streaming. A bug is making it so users are unable to enable HDR video streaming after upgrading to Windows 10 1903 or later if they previously disabled the setting. To fix this issue, Microsoft says you can perform one of two steps; roll back to Windows 10 1809, enable the setting, and then upgrade again or make a change in the Registry.

www.ke-cirt.go.ke