NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
28th May 2020

COMMUNICATIONS
AUTHORITY OF KENYA

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

Top Stories

Source 1 : The Jakarta Post (https://www.thejakartapost.com/)
https://www.thejakartapost.com/news/2020/05/28/hackers-breach-data-of-education-and-culture-ministrys-1-3-million-civil-servants.html?&web_view=true
Impact value: High
1.3 million users' data breached. The data of up to 1.3 million civil servants have been reportedly breached after unknown hackers infiltrated the Indonesian Education and Culture Ministry. The compromised data includes full names, citizenship identification numbers (NIK), Family Card numbers, home addresses, and birth dates of the affected individuals.

Source 2 : Cyber News (https://cybernews.com/)
https://cybernews.com/security/real-estate-app-leaking-thousands-of-user-records-and-sensitive-private-messages/
Impact value: High
Tellus app leaks data. An unsecured Amazon S3 bucket had leaked thousands of user records and private messages belonging to the Tellus app. The data bucket in question contained a folder with 6,729 CSV files related to the app. The leaky bucket was fixed after the company was made aware by researchers.

Source 3 : Threat Post (https://threatpost.com/)
https://threatpost.com/google-location-tracking-arizona-lawsuit/156082/
Impact value: Informative
Google Location Tracking Lambasted in Arizona Lawsuit. The lawsuit, filed against Google by Arizona's Attorney General, alleges that the tech giant uses "deceptive and unfair conduct" to obtain users' location data. Google has been hit by a lawsuit alleging that it violates user privacy by collecting location data via various means – and claiming that Google makes it nearly "impossible" for users to opt out of such data tracking.

System vulnerabilities

Source 1 : Threat Post (https://threatpost.com/)
https://threatpost.com/hackers-compromise-cisco-servers-saltstack/156091/
Impact value: Critical
Hackers Compromise Cisco Servers Via SaltStack Flaws. Cisco said attackers have been able to compromise its servers after exploiting two known, critical SaltStack vulnerabilities. The flaws exist in the open-source Salt management framework, which are used in Cisco network-tooling products. Cisco said the servers were remediated on May 7. The company also released software updates for the two vulnerable products. Cisco said that the update is "critical," ranking it 10 out of 10 on the CVSS scale.

Source 2 : Bleeping Computer (https://www.cybereason.com/)
https://www.bleepingcomputer.com/news/security/nsa-russian-govt-hackers-exploiting-critical-exim-flaw-since-2019/
Impact value: Critical
NSA: Russian govt hackers exploiting critical Exim flaw since 2019. The U.S. National Security Agency (NSA) says that Russian military threat actors known as Sandworm Team have been exploiting a critical flaw in the Exim mail transfer agent (MTA) software since at least August 2019. The vulnerability tracked as CVE-2019-10149 and named "The Return of the WIZard" makes it possible for unauthenticated remote attackers to execute arbitrary commands as root on vulnerable mail servers — for some non-default server configurations — after sending a specially crafted email.

Malware

Source 1 : Threat Post (https://threatpost.com/)
https://threatpost.com/funicorn-ransomwarecovid-19-contact-tracing-app/156069/
Impact value: High
*[F]Unicorn ransomware***.** Researchers have detected a new ransomware strain called [F]Unicorn that targets Italian users by masquerading as an official COVID-19 contact tracing app. Once the app is installed, it executes the ransomware in the background while showing a fake dashboard on COVID-19 to the user. After encrypting data, [F]Unicorn displays a ransom note, asking for 300 euros in exchange for the decryption key.

Source 2 : Cybereason (https://www.cybereason.com/)
https://www.cybereason.com/blog/valak-more-than-meets-the-eye
Impact value: High
Valak malware evolves. Recent versions of Valak malware have been found targeting Microsoft Exchange servers in a massive cyberespionage campaign. The primary goal of these malware versions is to steal targeted enterprises' mailing information and passwords along with their certificates. This campaign is specifically used against enterprises in the US and Germany.

Source 3 : Bleeping Computer (https://www.cybereason.com/)
https://www.bleepingcomputer.com/news/security/new-octopus-scanner-malware-spreads-via-github-supply-chain-attack/
Impact value: High
New Octopus Scanner malware spreads via GitHub supply chain attack. Security researchers have found a new malware that finds and backdoors open-source NetBeans projects hosted on the GitHub web-based code hosting platform to spread to Windows, Linux, and macOS systems and deploy a Remote Administration Tool (RAT).

Spam
&
Phishing

Source 1 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/cyber-criminals-impersonating/
Impact value: Medium
Google sites impersonated. According to a new report, threat actors impersonated different products of Google to launch 65,000 cyberattacks in the first four months of 2020. The purpose of these attacks was to steal login credentials from users. Most of these attacks involved the use of Google file sharing and storage services such as Google Docs, Google Drive, and Google Cloud storage.

Source 2 : Bleeping Computer (https://www.cybereason.com/)
https://www.bleepingcomputer.com/news/security/fake-valorant-mobile-app-pushes-scams-on-eager-gamers/
Impact value: Medium
Fake Valorant Mobile app pushes scams on eager gamers. As the eagerly anticipated tactical FPS game Valorant ends their closed beta, a fake mobile version is being distributed that displays nothing but scams to those who install it. This particular scam just displays affiliate offers, but there is nothing to stop a threat actor from also installing malware on an Android device.

Web Security

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

https://www.bleepingcomputer.com/news/security/minted-discloses-data-breach-after-5m-user-records-sold-online/

Impact value: Critical

Minted discloses data breach after 5M user records sold online. Minted, a US-based marketplace for independent artists, has disclosed a data breach after a hacker sold a database containing 5 million user records on a dark web marketplace. The information involved includes customers' names and login credentials to their Minted accounts, consisting of their email address and password. The passwords were hashed and salted and not in plain text. Telephone number, billing address, shipping address(es), and, for fewer than one percent of affected customers, date of birth, also may have been impacted

https://www.bleepingcomputer.com/news/security/200k-sites-with-buggy-wordpress-plugin-exposed-to-wipe-attacks/

Impact value: High

200K sites with buggy WordPress plugin exposed to wipe attacks. Two high severity security vulnerabilities found in the PageLayer plugin can let attackers to potentially wipe the contents or take over WordPress sites using vulnerable plugin versions. The vulnerabilities were reported to PageLayer's developer by the Wordfence Threat Intelligence team on April 30 and were patched with the release of version 1.1.2 on May 6. According to Wordfence, the two security flaws can be exploited by attackers to wipe WordPress sites running older unpatched versions of the plugin, as well as launch takeover attacks.

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: Critical
SaltStack FrameWork Vulnerabilities Affecting Cisco Products. On April 29, 2020, the Salt Open Core team notified their community regarding the following two CVE-IDs: CVE-2020-11651: Authentication Bypass Vulnerability and CVE-2020-11652: Directory Traversal Vulnerability. Cisco Modeling Labs Corporate Edition (CML) and Cisco Virtual Internet Routing Lab Personal Edition (VIRL-PE) incorporate a version of SaltStack that is running the salt-master service that is affected by these vulnerabilities. Cisco has released software updates that address these vulnerabilities. There is a workaround that addresses these vulnerabilities.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/all-the-security-features-added-in-the-windows-10-may-2020-update/
Impact value: Informative
All the security features added in the Windows 10 May 2020 update. The Windows 10 May 2020 update, also known as Windows 10 2004, has started rolling out to users today. This Windows 10 2004 version also comes with improvements on the security front, which Microsoft claims will help keep Windows 10 users safe going forward.

www.ke-cirt.go.ke