NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
7th June 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	1	0
System Vulnerabilities	2	0	0	0
Malware	0	4	1	0
DDoS/Botnets	0	0	0	0
Spam & Phishing	0	0	1	1
Web Security	0	1	1	0
Updates & Alerts	0	1	0	1

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1 : Bleeping Computer (https://www.cybereason.com/)
https://www.bleepingcomputer.com/news/security/cpa-canada-discloses-data-breach-affecting-329-000-individuals/?&web_view=true
Impact value: High
CPA Canada discloses data breach. The Chartered Professional Accountants of Canada (CPA) has fallen victim to a security breach that affected the personal information of over 329,000 members and other stakeholders. The compromised information includes both employer and employee names and addresses.

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/whatsapp-phone-numbers-google-search-results/156141/
Impact value: Medium
WhatsApp Phone Numbers Pop Up in Google Search Results. A researcher is warning that a WhatsApp feature called "Click to Chat" puts users' mobile phone numbers at risk — by allowing Google Search to index them for anyone to find. But WhatsApp owner Facebook says it is no big deal and that the search results only reveal what the users have chosen to make public anyway.

Source 3 : Bleeping Computer (https://www.cybereason.com/)
https://www.bleepingcomputer.com/news/security/fitness-depot-hit-by-data-breach-after-isp-fails-to-activate-the-antivirus/
Impact value: High
Fitness Depot hit by data breach after ISP fails to 'activate the antivirus'. Canadian retailer Fitness Depot announced customers that their personal and financial information was stolen following a breach that affected the company's e-commerce platform last month. Fitness Depot is the largest specialty exercise equipment retailer in Canada, with 40 stores nationwide and two in the United States, Texas, in Dallas and Houston.

System vulnerabilities

Source 1 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/critical-vulnerability-could-have-allowed-hackers-disrupt-traffic-lights
Impact value: Critical
Vulnerable traffic light controller. Traffic light controllers made by SWARCO are affected by a critical vulnerability that could be exploited by hackers to disrupt a city's traffic lights. The flaw, tracked as CVE-2020-12493, has a CVSS score of 10. The affected model is CPU LS4000. Swarco has patched the flaw soon after it was made aware by researchers.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/windows-10-smbghost-bug-gets-public-proof-of-concept-rce-exploit/
Impact value: Critical
Windows 10 SMBGhost bug gets public proof-of-concept RCE exploit. Working exploit code that achieves remote code execution on Windows 10 machines is now publicly available for CVE-2020-0796, a critical vulnerability in Microsoft Server Message Block (SMB 3.1.1). More refined versions of the exploit are expected to emerge, especially since at least two cybersecurity companies created exploits for the vulnerability and have been holding back the release since April. Known by various names (SMBGhost, CoronaBlue, NexternalBlue, BluesDay), the security flaw can be leveraged by an unauthenticated attacker to spread malware from one vulnerable system to another without user interaction.

Malware

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

https://www.bleepingcomputer.com/news/security/ongoing-ech0raix-ransomware-campaign-targets-qnap-nas-devices/

Impact value: High

Ongoing eCh0raix ransomware campaign targets QNAP NAS devices. After remaining relatively quiet over the past few months, the threat actors behind the eCh0raix Ransomware have launched a brand new campaign targeting QNAP storage devices. eCh0raix was first seen in June 2019, after victims began reporting ransomware attacks in a forum topic on BleepingComputer. On June 1st, 2020, there has been a sudden surge of eCh0raix victims seeking help in our forums and submissions to the ransomware identification site ID-Ransomware.

https://www.bleepingcomputer.com/news/security/us-aerospace-services-provider-breached-by-maze-ransomware/

Impact value: High

US aerospace services provider breached by Maze Ransomware. The Maze Ransomware gang breached and successfully encrypted the systems of VT San Antonio Aerospace, as well as stole and leaked unencrypted files from the company's compromised devices in April 2020. VT San Antonio Aerospace (VT SAA) is a leading North American aircraft MRO (maintenance, repair, and overhaul) service provider specialized in airframe maintenance repair and overhaul, line maintenance, aircraft modifications, and aircraft engineering services.

Malware

https://www.bleepingcomputer.com/news/security/fake-ransomware-decryptor-double-encrypts-desperate-victims-files/

Impact value: High

Fake ransomware decryptor double-encrypts desperate victims' files. A fake decryptor for the STOP Djvu Ransomware is being distributed that lures already desperate people with the promise of free decryption. Instead of getting their files back for free, they are infected with another ransomware that makes their situation even worse.

Source 2 : Blackberry (https://blogs.blackberry.com/)

https://blogs.blackberry.com/en/2020/06/threat-spotlight-tycoon-ransomware-targets-education-and-software-sectors

Impact value: High

Tycoon ransomware. Security researchers have uncovered a new ransomware strain, Tycoon, that is deployed in the form of a trojanized Java Runtime Environment (JRE). It leverages an obscure Java image format to evade detection. The ransomware uses the AES-256 algorithm with a 16-byte long GCM authentication tag to encrypt files.

Source 3 : Trend Micro (https://blog.trendmicro.com/)

https://blog.trendmicro.com/trendlabs-security-intelligence/barcode-reader-apps-on-google-play-found-using-new-ad-fraud-technique/?web_view=true

Impact value: Medium

Malicious apps. Two malicious barcode reader apps - Barcode Reader and QR&Barcode Scanner - were removed from the Google Play Store, following the detection of suspicious activities. These apps forced users to run ads every 15-minutes while running malicious activities in the background. This caused the phone screens to crash.

Spam & Phishing

Source 1 : Bleeping Computer (https://www.cybereason.com/)
https://www.bleepingcomputer.com/news/security/100-000-company-inboxes-hit-with-voice-message-phishing/
Impact value: Medium
100,000 company inboxes hit with voice message phishing. Attackers have been pounding employee inboxes at companies that still use private branch eXchange (PBX) telephone systems for communication, delivering phishing that bypasses email defenses. The messages pretended to be voicemail notifications from PBX integrations and featured custom subject lines to pass a superficial legitimacy test.

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/electrolux-conned-money-bec-scammer/156359/
Impact value: Informative
Electrolux, Others Conned Out of Big Money by BEC Scammer. A 64-year-old business email compromise (BEC) guru has plead guilty in Houston to bilking appliance giant Electrolux and one other company out of a combined half a million dollars — in addition to other fraud schemes. Kenenty Hwan Kim (a.k.a. Myung Kim) admitted in federal court (the Southern District of Texas) that he had carried out the elaborate schemes, which involved spoofed emails that purported to be internal communications from executives at the target companie

Web Security

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
bleepingcomputer.com/news/security/hackers-tried-to-steal-database-logins-from-13m-wordpress-sites/

Impact value: Medium

Hackers tried to steal database logins from 1.3M WordPress sites. A large scale attack targeted hundreds of thousands of WordPress websites over the course of 24 hours, attempting to harvest database credentials by stealing config files after abusing known XSS vulnerabilities in WordPress plugins and themes. "Between May 29 and May 31, 2020, the Wordfence Firewall blocked over 130 million attacks intended to harvest database credentials from 1.3 million sites by downloading their configuration files," Wordfence QA engineer and threat analyst Ram Gall said.

https://www.bleepingcomputer.com/news/security/zee5-allegedly-hacked-by-korean-hackers-customer-info-at-risk/

Impact value: High

ZEE5 allegedly hacked by 'Korean hackers', customer info at risk. A hacker identifying themselves as "John Wick" and "Korean Hackers" claim to have breached the systems for Indian video on demand giant ZEE5 and are threatening to sell the database on criminal markets. ZEE5 is an Indian streaming service with over 150 million subscribers worldwide and is part of the Essel Group conglomerate, the same company that owns ZEE news media outlets and TV channels. Earlier this year, a paste floating on the web exposed credentials of some 1,023 Premium ZEE5 accounts. After reporting these accounts to ZEE5, they were quick to respond, but we are not aware of notifications sent to affected accounts.

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 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/ublock-origin-for-chrome-now-blocks-port-scans-on-most-sites/
Impact value: Informative
uBlock Origin for Chrome now blocks port scans on most sites. A recent update to an ad block filter list now allows the uBlock Origin extension to block most of the known sites that perform port scans of your local Windows computer. This comes after a few weeks ago, when it was reported that eBay is using fraud detection scripts that port scan a visitor's computer for Windows remote access programs. Another report followed showing how eleven other sites were port scanning their visitors after cybersecurity intelligence firm DomainTools shared a list of domains utilizing the fraud detection scripts.

Source 2 : Secure Zoo (https://www.securezoo.com/)
https://www.securezoo.com/2020/06/google-releases-chrome-security-update-83-0-4103-97/
Impact value: High
Chrome 83.0.4103.97 released. Google has released Chrome 83.0.4103.97 for Windows, Mac, and Linux Operating Systems. This latest update addresses five security flaws, out of which four are high-severity vulnerabilities. In addition to this, Google has also addressed two medium-severity vulnerabilities, tracked as CVE-2020-6497 and CVE-2020-6498, in Chrome 83.0.4103.88 for the iOS release.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke