NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
11th 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	0	1
System Vulnerabilities	2	2	0	0
Malware	0	3	0	0
DDoS/Botnets	0	1	0	0
Spam & Phishing	0	2	0	0
Web Security	0	2	0	0
Updates & Alerts	0	0	2	1

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/
Impact value: High
A1 Telekom disclosed a hack. Austria's largest internet service provider, A1 Telekom, admitted falling victim to a cyberattack in November 2019. The hack was believed to be the work of the China-based Gallium threat actor group. It took six months for the firm to restore its infected systems and servers.

Source 2 : SC Magazine (https://www.scmagazine.com/)
https://www.scmagazine.com/home/security-news/babylon-health-glitch-allowed-app-users-access-to-others-video-consults/
Impact value: High
Flawed app reveals data. A glitch in the Babylon Health app allowed users to gain access to other users' video consultations with doctors. The flaw was addressed on June 9 after the telehealth company was informed by a user.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/hackers-are-quick-to-notice-exposed-elasticsearch-servers/
Impact value: Informative
Hackers are quick to notice exposed Elasticsearch servers. Bad guys find unprotected Elasticsearch servers exposed on the web faster than search engines can index them. A study found that threat actors are mainly going for cryptocurrency mining and credential theft. For the duration of the experiment, a honeypot with a fake database recorded more than 150 unauthorized requests, the first one occurring less than 12 hours since being exposed.

System vulnerabilities

Source : Security Week (https://www.securityweek.com/)

https://www.securityweek.com/details-released-recently-patched-code-execution-vulnerability-firefox

Impact value: High

Details of an RCE flaw released. Cisco's Talos threat intelligence and research group has released details about a recently patched code execution vulnerability in Firefox. The flaw, tracked as CVE-2020-12405, features a CVSS score of 8.8 and can be exploited when the user navigates to a malicious page. It was fixed with the release of Firefox 77.

https://www.securityweek.com/critical-vulnerability-patched-sap-commerce

Impact value: Critical

SAP patches flaw. SAP has addressed a total of 19 vulnerabilities as part of its June 2020 Patch Tuesday. Out of these, two are rated 'Critical'. These flaws are identified as CVE-2020-1938 and CVE-2020-6265 and have a CVSS score of 9.8.

https://www.securityweek.com/google-researcher-finds-vulnerability-vmware-virtualization-products

Impact value: High

VMware issues patches. VMware has patched a high-severity information disclosure vulnerability affecting its Workstation, Fusion, and vSphere virtualization products. The flaw is tracked as CVE-2020-3960 and could allow attackers with non-admin access to a machine to read privileged information from memory.

https://www.securityweek.com/smbleed-vulnerability-impacts-windows-smb-protocol

Impact value: Critical

SMBleed patched. Microsoft's June 2020 Security Updates includes a fix for a Server Message Block (SMB) protocol bug that could allow attackers to leak kernel memory remotely without authentication. Called SMBleed and tracked as CVE-2020-1206, the flaw is linked to SMBGhost which was addressed in March 2020.

Malware

Source 1 : Microsoft (https://www.microsoft.com/)
https://www.microsoft.com/security/blog/2020/06/10/misconfigured-kubeflow-workloads-are-a-security-risk/

Impact value: High

XMRig installed. Microsoft has revealed a series of attacks against Kubeflow, a toolkit for running Machine Learning (ML) operations on Kubernetes clusters. The attacks, which are active since April this year, are being carried out to install an XMRig miner on vulnerable Kubernetes clusters. The attackers are taking advantage of publicly exposed Kubeflow management panel to launch these attacks.

Source 2 : Dark Reading (https://www.darkreading.com/)
https://www.darkreading.com/vulnerabilities---threats/fake-covid-19-contact-tracing-apps-infect-android-phones/d/d-id/1338047?&web_view=true

Impact value: High

Fake contact-tracing apps. Researchers have traced 12 malicious contact-tracing apps that contain a wide range of malware, including Anubis and SpyNote. These apps are likely being distributed via other mobile apps, third-party stores, and websites, among other sources. Researchers learned that these apps are targeting citizens across multiple countries.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/city-of-knoxville-shuts-down-network-after-ransomware-attack/

Impact value: High

City of Knoxville shuts down network after ransomware attack. The City of Knoxville, Tennessee, was forced to shut down its entire computer network following a ransomware attack that took place overnight and targeted the city's offices. Computers on Knoxville's network were encrypted overnight, with the attack being noticed by employees of the city's fire department around 4:30 AM, June 11, according to Chief Operations Officer David Brace.

Botnets/DDoS

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/kingminer-botnet-brute-forces-mssql-databases-to-install-cryptocurrency-miner/

Impact value: High

KingMiner botnet returns. Security researchers have detected a new KingMiner botnet operation that targets MSSQL databases with brute-force attacks. Once hackers break into a vulnerable MSSQL system, they create another database user named ‘dbhelp’ and install a cryptocurrency miner that abuses the server’s resources to generate profits for the gang.

Spam & Phishing

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/fake-black-lives-matter-voting-campaign-spreads-trickbot-malware/

Impact value: High

TrickBot returns. A phishing email campaign asking recipients to vote anonymously on Black Lives Matter has been found spreading the TrickBot trojan. The subject line of the email states, “Leave a review confidentially about 'Black Lives Matter’. It prompts the recipients to fill out and return an attached document named ‘e-vote_form_3438.doc.’

Source 3 : Abnormal Security (https://abnormalsecurity.com/)
https://abnormalsecurity.com/blog/abnormal-attack-stories-covid-19-relief-phishing-through-dropbox-transfer/

Impact value: High

Microsoft Office 365 users targeted. Business owners with Microsoft Office 365 accounts are being targeted in a phishing email campaign that appears to come from the U.K government. These emails claim to offer financial relief announced by the government to small businesses. Attached in the emails is a link to a COVID-19-Relief-Payment.PDF document, which if clicked, redirects the users to a benign Dropbox Transfer landing page. The purpose of the scam is to steal personal details of individuals.

Web Security

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

https://www.bleepingcomputer.com/news/security/live-event-solutions-leader-tait-discloses-data-breach/

Impact value: High

Live event solutions leader TAIT discloses data breach. TAIT, one of the world's leading live event solutions providers, disclosed a data breach that led to the exposure of personal and financial information stored on a server and on the email accounts of some of its employees. The TAIT group of companies (Brilliant, Kinesys, Production Glue, Stage Technologies, TAIT UK, and TAIT Navigator) employs over 900 people in 14 office locations around the world and has been a provider of live experience solutions in over 30 countries, on all seven continents.

https://www.bleepingcomputer.com/news/security/fortune-500-insurance-firm-genworth-discloses-data-breach/

Impact value: High

Fortune 500 insurance firm Genworth discloses data breach. Fortune 500 insurance holding company Genworth Financial disclosed a data breach after an unauthorized party gained access to insurance agents' online accounts using compromised login credentials. The data breach was discovered by Genworth on April 20, 2020, after the company detected unauthorized access to some insurance agents' online accounts, providing access to documents containing both personal and financial information.

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 : Cisco (https://tools.cisco.com/)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tcl-dos-MAZQUnMF

Impact value: Medium

Cisco IOS and IOS XE Software Tcl Denial of Service Vulnerability. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-pi-xss-12713

Impact value: Medium

Cisco Prime Infrastructure Cross-Site Scripting Vulnerability. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.

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

https://www.bleepingcomputer.com/news/security/new-windows-10-smbv3-flaw-can-be-used-for-data-theft-rce-attacks/

Impact value: Informative

Android 11 brings numerous security and privacy improvements. The beta version of Android 11, the next version of Google's operating system for mobile devices, comes with lots of security and privacy changes designed to allow the OS to protect users' data from malicious attacks. On the privacy side, the new Android release will come with one-time permissions, automated permissions reset, and scope storage enforcement.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke