NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
25th 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	0
System Vulnerabilities	0	2	0	0
Malware	0	2	0	0
DDoS/Botnets	0	1	0	0
Spam & Phishing	0	1	1	0
Web Security	0	2	0	0
Updates & Alerts	1	0	0	1

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/online-education-site-educba-discloses-data-breach-after-hack/

Impact value: High

Online education site EduCBA discloses data breach after hack. EduCBA has started notifying customers that they are resetting their passwords after suffering a data breach. EduCBA is an online education site based out of India that offers over 2,500 online courses and job oriented learning programs focus on finance, technology, and business to their 500,000 learners. On Saturday, EduCBA began emailing data breach notifications to customers stating that their systems were hacked and user data was exposed.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/thousands-of-enterprise-systems-infected-by-new-blue-mockingbird-malware-gang/

Impact value: High

Thousands of enterprise systems infected by new Blue Mockingbird malware gang. Thousands of enterprise systems are believed to have been infected with a cryptocurrency-mining malware operated by a group tracked under the codename of Blue Mockingbird. Discovered earlier this month by malware analysts from cloud security firm Red Canary, the Blue Mockingbird group is believed to have been active since December 2019.

System vulnerabilities

Source 1 : Threat Post (https://threatpost.com/)
https://www.bleepingcomputer.com/news/security/hackers-leak-credit-card-info-from-costa-ricas-state-bank/
Impact value: High
70 Percent of Mobile, Desktop Apps Contain Open-Source Bugs. A full 70 percent of applications being used today have at least one security flaw stemming from the use of an open-source library. According to Veracode's annual State of Software Security report, these open-source libraries – free, centralized code repositories that provide ready-made application "building blocks" for developers – are not only ubiquitous but also risky.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/new-unc0ver-jailbreak-released-works-on-all-recent-ios-versions/
Impact value: High
New Unc0ver jailbreak released, works on all recent iOS versions. A team of hackers, security researchers, and reverse engineers have released today a new jailbreak package for iOS devices. This is possible, they said, because Unc0ver 5.0.0 utilizes a zero-day vulnerability in the iOS operating system, a vulnerability that Apple is not aware of. The zero-day was discovered by one of Unc0ver's members, a hacker known as Pwn20wnd.

Malware

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

https://www.bleepingcomputer.com/news/security/discord-client-turned-into-a-password-stealer-by-updated-malware/

Impact value: High

Discord client turned into a password stealer by updated malware. A threat actor updated the AnarchyGrabber trojan into a new version that steals passwords and user tokens, disables 2FA, and spreads malware to a victim's friends. AnarchyGrabber is a popular trojan that is commonly spread for free on hacker forums and within YouTube videos that explain how to steal Discord user tokens. Threat actors then distribute the trojan on Discord, where they pretend it's a game cheat, hacking tool, or copyrighted software.

https://www.bleepingcomputer.com/news/security/hacker-extorts-online-shops-sells-databases-if-ransom-not-paid/

Impact value: High

Hacker extorts online shops, sells databases if ransom not paid. More than two dozen SQL databases stolen from online shops in various countries are being offered for sale on a public website. In total, the seller provides over 1.5 million rows of records but the amount of stolen data is much larger. The attacker is hacking into insecure servers that are reachable over the public web, copies the databases, and leaves a note asking for a ransom in return of the stolen data.

Botnets/DDoS

Source 1 : Cyware (https://cyware.com/)
https://cyware.com/news/large-scale-ddos-attack-techniques-evolve-further-cea46b98
Impact value: High
Large-Scale DDoS Attack Techniques Evolve Further. Attackers have been using new and innovative methods to target their victim's infrastructure through DDoS attacks. NXNSAttack is yet another method, that can cause havoc on the targeted victim's networks.

Spam & Phishing

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/coronavirus-emails-netsupport-rat-microsoft/156026/
Impact value: High
'Coronavirus Report' Emails Spread NetSupport RAT, Microsoft Warns. A recent spear-phishing campaign has been spotted spreading a weaponized NetSupport Manager remote access tool (RAT), which is a legitimate tool used for troubleshooting and tech support. Attackers use the ongoing coronavirus pandemic as a lure, as well as malicious Excel documents, to convince victims to execute the RAT.

Source 3 : Cyware (https://cyware.com/)
https://cyware.com/news/scammers-use-contact-tracing-as-bait-to-target-users-78727a6d
Impact value: Medium
Scammers Use Contact Tracing as Bait to Target Users. As scammers usually do their homework and are aware of the latest developments in the pandemic, they are now posing as contact tracers to target their victims. The scammers are sending phony text messages asking recipients to click on a scammy link and share their personal details as they have come in contact with a person who tested positive for COVID-19

Web Security

Source 1 : Threat Post (https://threatpost.com/)
https://threatpost.com/home-chef-data-breach-8-million-records/156031/
Impact value: High
Home Chef Serves Up Data Breach for 8 Million Records. According to a notice posted on the Home Chef website, the company "recently learned of a data security incident impacting select customer information." That info includes email addresses, names, phone numbers, encrypted passwords and the last four digits of credit-card numbers.

Source 2 : Yahoo (https://in.finance.yahoo.com/)
https://in.finance.yahoo.com/news/cyber-criminals-leak-personal-data-180107569.html?&web_view=true
Impact value: High
Cyber criminals leak personal data of 29 million Indians on dark web for free. Cyber criminals have posted personal data of 29 million job-seeking Indians on dark web for free in one of the hacking forums, according to online intelligence firm Cyble. The cyber intelligence firm said that the breach includes sensitive information such as email, phone, home address, qualification, work experience etc.

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-uccx-rce-GMSC6RKN

Impact value: Critical

Cisco Unified Contact Center Express Remote Code Execution Vulnerability. The vulnerability is due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a malicious serialized Java object to a specific listener on an affected system. A successful exploit could allow the attacker to execute arbitrary code as the root user on 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