NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
9th June 2020

COMMUNICATIONS AUTHORITY OF KENYA

Summary Headlines	Impact Metric Against Count of Events			
	Critical	High	Medium	Informative
Regional Highlights	0	0	0	2
Top Stories	0	3	0	0
System Vulnerabilities	2	0	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

Regional Highlights

Source 1 : The Standard (https://www.standardmedia.co.ke/)
https://www.standardmedia.co.ke/business/article/2001374455/digital-lenders-under-fire-over-shaming-loan-defaulters

Impact value: Informative

Digital lenders criticized over reaching out to defaulters' relatives, bosses. This came out following online protests over how the operators namely Opesa and Okash deploy unpopular ways to get back their money from defaulters. The association on Monday said it has taken note with great concern the continued reports about Opesa and Okash's poor shaming practices of debt collection whereby they reach out to contacts on the customer's phone book to try and get them to pay back a loan. "Not only does this behaviour go against Kenyan data protection laws, but it reeks of indignity. By reaching out to a customer's contact list, Opesa and Okash rob the individual of basic dignity and consumer rights. This can have long term effects on their psychological well-being and damage relations that may have taken years to build," said DLAK Chairman Robert Masinde on behalf of all members.

Source 2 : Techweez (https://techweez.com/)
https://techweez.com/2020/06/09/netflix-users-in-kenya-soar/

Impact value: Informative

Netflix Users in Kenya Have Surged Over 700% in the Last 3 Years. Netflix was launched in Kenya in 2016 as part of the global expansion the streaming giant did in that year. It was their big switch from being present in a few countries and enabled Kenyans to enjoy content easily on their site. According to Statista, the estimated number of active streaming subscribers to Netflix in Kenya has risen from around 3600 in 2017 to over 29,500 in 2020. That's a 700% increase in 3 years and it shows the explosive growth of the use of the streaming site in Kenya.

Top Stories

Source 1 : The Daily Swig (https://portswigger.net/)
https://portswigger.net/daily-swig/south-african-healthcare-provider-hit-by-cyber-attack
Impact value: High
Life Healthcare attacked. The South Africa-based Life Healthcare is investigating a cyberattack that affected some of the group's IT systems. According to the organization, it immediately took systems offline to contain the incident. It is yet to ascertain the extent to which sensitive data has been compromised.

Source 2 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/ransomware-strikes-third-us/
Impact value: High
Columbia College hit. Columbia College is the third US college to have fallen victim to a cyberattack by Netwalker ransomware operators. The attack had occurred on June 3 and had resulted in the compromise of sensitive data like social security numbers.

Source 3 : Threat Post (https://threatpost.com/)
https://threatpost.com/dark-basin-hack-hire-group/156407/
Impact value: High
Dark Basin Hack-For-Hire Group Targeted Thousands Over 7 Years. A hack-for-hire group, called Dark Basin, has been outed after targeting thousands of individuals and organizations worldwide – including advocacy groups and journalists, elected and senior government officials, and hedge funds — over the course of seven years. In all, more than 10,000 victim email accounts were targeted, according to Reuters, who broke the news.

System vulnerabilities

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

https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-remote-code-execution-bug-in-flash-player/

Impact value: Critical

Adobe fixes critical remote code execution bug in Flash Player. Adobe has released security updates for Adobe Flash Player, Adobe Experience Manager, and Adobe Framemaker that fix ten security vulnerabilities in the three products. Of the ten vulnerabilities, four are classified as 'Critical' as they allow an attacker to remotely execute commands on vulnerable systems. If you use any of these products, it is strongly suggested that you upgrade to the latest versions as soon as possible.

https://www.bleepingcomputer.com/news/security/intel-patched-22-vulnerabilities-in-the-june-2020-platform-update/

Impact value: Critical

Vulnerabilities in popular open source projects doubled in 2019. Intel addressed 25 vulnerabilities today as part of its June 2020 Patch Tuesday, with two of them affecting Intel's Active Management Technology (AMT) being rated as critical security flaws after receiving CVSS scores of 9.8. These issues were detailed in the five security advisories Intel published on its Product Security Center, with fixes addressing them having been delivered to users through the Intel Platform Update (IPU) process before public disclosure.

Malware

Source 1 : RISKIQ (https://www.riskiq.com/)
https://www.riskiq.com/blog/labs/misconfigured-s3-buckets/
Impact value: High
Jqueryapi1oad. New details related to a Magecart attack campaign carried out through misconfigured S3 buckets have emerged lately. It has been found that along with the skimming code, the compromised buckets were also used for delivering a malicious redirector, referred to as 'jqueryapi1oad'. The malware is linked to a long-running Hookads malvertising campaign. So far, the 277 sites have been identified as affected by jqueryapi1oad malware.

Source 2 : ProofPoint (https://www.proofpoint.com/)
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
Impact value: High
FlowCloud malware. Researchers have discovered a new modular malware named FlowCloud that was used against U.S. utility providers in August 2019. The malware shares similarities with LookBack malware and enables its operators to take complete control over a compromised system. Its capabilities include accessing installed applications, the keyboard, mouse, screen, files, services, and processes on an infected system.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/valak-malware-gets-new-plugin-to-steal-outlook-login-credentials/
Impact value: High
Valak malware gets new plugin to steal Outlook login credentials. Authors of Valak information stealer are focusing more and more on stealing email credentials as researchers find a new module specifically built for this purpose. The malware emerged in testing mode in mid-October 2019 and has a modular plugin architecture that expands its capabilities to cover the needs of the threat actor.

Botnets/DDoS

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/callstranger-vulnerability-lets-attacks-bypass-security-systems-and-scan-lans/

Impact value: High

CallStranger vulnerability can also be used to launch major DDoS attacks. A severe vulnerability, dubbed CallStranger, residing in the UPnP protocol can allow attackers to hijack smart devices and launch DDoS attacks. Additionally, the flaw can enable attackers to successfully bypass network security solutions and firewalls. The CallStranger flaw is tracked as CVE-2020-12695.

Spam & Phishing

Source 2 : Security Intelligence (https://securityintelligence.com/)
https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

Impact value: High

Credential harvesting attack. A large-scale phishing campaign targeting high-profile executives of German multinational corporations associated with the task of procuring PPE kit, has come to notice. So far, the cybercrooks have attempted to steal credentials of more than 100 senior executives working in 40 different organizations. Some of the targeted organizations include FIEGE, Deutsche Bahn, Bayer, Daimler, DHL, Lufthansa, Otto, and Volkswagen.

Source 3 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/new-hmrc-phishing-scam?utm_source=twitterfeed&utm_medium=twitter

Impact value: High

HMRC impersonated. The phishing email informs victims that they are eligible for a tax rebate from Her Majesty's Revenue and Customs (HMRC). It redirects the victims to a fake HMRC site which asks them to enter their email address, postcode, and HMRC login details. In order to get the promised refund amount, they are further asked to enter their card number, name on card, account numbers, security code, and expiry date.

Web Security

Source 1 : Tech (https://tech.economictimes.indiatimes.com/)
https://tech.economictimes.indiatimes.com/news/internet/bemls-internal-data-and-employee-credentials-leaked-on-dark-web-report/76279224?&web_view=true
Impact value: High
BEML's internal data and employee credentials leaked on dark web. Internal documents of defence public sector undertaking BEML (Bharat Earth Movers Limited) have been leaked on marketplaces in the dark web, US-based cybersecurity research firm Cyble said on Tuesday. The actual leak of the documents took place on May 25, it said, suspecting that a hacktivist or a Pakistan-based threat actor called 'R3dr0x' has targeted the website and leaked sensitive data files along with email accounts and passwords of seven employees.

Source 2 : Los Angeles Times (https://www.latimes.com/)
https://www.latimes.com/world-nation/story/2020-06-09/paid-hackers-dark-basin-targeted-thousands-people-hundreds-institutions?&web_view=true
Impact value: High
Paid hackers targeted thousands of people and hundreds of institutions worldwide. Researchers discovered almost 28,000 web pages created by hackers for personalized "spear phishing" attacks designed to steal passwords, according to a report published Tuesday by Citizen Lab, part of the University of Toronto's Munk School.

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/microsoft/microsoft-june-2020-patch-tuesday-largest-ever-with-129-fixes/

Impact value: Informative

Microsoft June 2020 Patch Tuesday: largest ever with 129 fixes. With the release of the June 2020 Patch Tuesday security updates, Microsoft has released one advisory for an Adobe Flash Player update and fixes for 129 vulnerabilities in Microsoft products. Of these vulnerabilities, 11 are classified as Critical, 109 as Important, 7 as Moderate, and 2 as Low.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke