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

Top Stories

Source 1 : The New York Times (https://www.nytimes.com/)
https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html?&web_view=true
Impact value: High
U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks. The F.B.I. and the Department of Homeland Security are preparing to issue a warning that China's most skilled hackers and spies are working to steal American research in the crash effort to develop vaccines and treatments for the coronavirus. The efforts are part of a surge in cybertheft and attacks by nations seeking advantage in the pandemic.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/texas-courts-hit-by-ransomware-network-disabled-to-limit-spread/
Impact value: High
Texas Courts hit by ransomware, network disabled to limit spread. The Texas court system was hit by ransomware on Friday night, May 8th, which led to the branch network including websites and servers being disabled to block the malware from spreading to other systems.

Source 3 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/iran-reports-failed-cyber-attack-on-strait-of-hormuz-port/
Impact value: Medium
Iran reports failed cyber-attack on Strait of Hormuz port. Iranian officials said on Sunday that hackers damaged a small number of computers in a failed cyber-attack against the port of Bandar Abbas, the country's largest port in the Strait of Hormuz. When the attack took place, local officials from the Ports and Maritime Organization (PMO) in the state of Hormozgan denied that anything had gone wrong.

System vulnerabilities

Source 1 : Helpnet Security (https://www.helpnetsecurity.com/)
https://www.helpnetsecurity.com/2020/05/11/cve-2020-12720/?web_view=true
Impact value: Critical
vBulletin fixes critical vulnerability, patch immediately! If you're using vBulletin to power your online forum(s), you should implement the newest security patches offered by the developers as soon as possible. The patches fix CVE-2020-12720, a vulnerability affecting versions 5.5.6, 5.6.0 and 5.6.1 with could be exploited without previous authentication. CVE-2020-12720 has been defined as an incorrect access control issue, but no additional information has been shared.

Source 2 : CISO (https://ciso.economictimes.indiatimes.com/)
https://ciso.economictimes.indiatimes.com/news/hacker-exposes-loopholes-in-mp-covid-19-dashboard/75667675
Impact value: High
Hacker exposes loopholes in MP Covid-19 dashboard. Four days after challenging the much hyped Aarogya Setu app, French cyber security researcher Robert Baptiste — who goes by the pseudonym Elliot Alderson on Twitter — forced the Madhya Pradesh government to "rework" its Covid-19 dashboard. The ethical hacker showed in his tweet the IDs of some of the patients, the districts they belong to, and the details of their devices, but cloaked their names and locations.

Source 3 : Threat Post (https://threatpost.com/)
https://threatpost.com/sphinx-riddle-us-targets-modifications/155621/
Impact value: High
Millions of Thunderbolt-Equipped Devices Open to 'ThunderSpy' Attack. A new attack enables bad actors to steal data from Windows or Linux devices equipped with Thunderbolt ports. If an attacker can get his hands on a Thunderbolt-equipped device for five minutes, he can launch a new data-stealing attack called "Thunderspy."

Malware

Source 1 : Cyware (https://cyware.com/)

https://cyware.com/news/the-next-wave-of-mobile-banking-threats-is-already-here-e8695415

Impact value: High

The Next Wave of Mobile Banking Threats Is Already Here. Mobile banking threats have been recently making an impact, both at the regional as well as global levels. EventBot, the newly identified Android banking trojan, can be considered as a forward leap in the evolution of mobile banking trojans.

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

https://www.bleepingcomputer.com/news/security/maze-ransomware-fails-to-encrypt-pitney-bowes-steals-files/

Impact value: High

Maze ransomware fails to encrypt Pitney Bowes, steals files. Global business services company Pitney Bowes recently stopped an attack from Maze ransomware operators before the encryption routine could be deployed but the actor still managed to steal some data. This attack comes less than months since the company recovered from another ransomware attack, with Ryuk, which was announced on October 14.

https://www.bleepingcomputer.com/news/security/north-korean-hackers-infect-real-2fa-app-to-compromise-macs/

Impact value: High

North Korean hackers infect real 2FA app to compromise Macs. Hackers have hidden malware in a legitimate two-factor authentication (2FA) app for macOS to distribute Dacls, a remote access trojan associated with the North Korean Lazarus group. Dacls has been used to target Windows and Linux platforms and the recently discovered RAT variant for macOS borrows from them much of the functionality and code.

Botnets/DDoS

Source 1 : Cisco (https://tools.cisco.com/)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wlc-dos
Impact value: High

Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability. A vulnerability in the web interface of Cisco Wireless LAN Controller Software could allow a low-privileged, authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

Spam & Phishing

Source 2 : Cyware (https://cyware.com/)
https://cyware.com/news/phishing-campaigns-threatens-users-with-fear-of-disruption-of-essential-services-c4173721
Impact value: Medium

Phishing Campaigns Threatens Users With Fear of Disruption of Essential Services. Hackers have been using fake messages related to essentials services to craft their scams. They often pose as a service provider and threaten the victims about the discontinuation of essential services if immediate action is not taken by the user. The Italian postal service provider Poste Italiane is the latest one to be added to the list of such lures used by hackers.

Source 3 : Threat Post (https://threatpost.com/)
https://threatpost.com/sphinx-riddle-us-targets-modifications/155621/
Impact value: Medium

Sphinx Malware Returns to Riddle U.S. Targets. The Zeus Sphinx banking trojan has seen a recent resurgence in the United States, sporting some modifications and using COVID-19 spam as a lure. The banking trojan has upgraded and is seeing a resurgence on the back of coronavirus stimulus payment themes.

Web Security

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/wordpress-plugin-bugs-can-let-hackers-take-over-almost-1m-sites/
Impact value: High
WordPress plugin bugs can let hackers take over almost 1M sites. Two high severity vulnerabilities found in the Page Builder WordPress plugin installed on more than 1,000,000 sites can let hackers create new admin accounts, plant backdoors, and ultimately take over the compromised websites. The vulnerabilities are a Cross-Site Request Forgery (CSRF) leading to Reflected Cross-Site Scripting (XSS) attacks and they affect all Page Builder versions up to and including 2.10.15.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/data-leak-phishing-security-flaws-exposed-in-oracle-iplanet-web-server/
Impact value: High
Data leak, phishing security flaws disclosed in Oracle iPlanet Web Server. Tracked as CVE-2020-9315 and CVE-2020-9314, the security flaws allow for sensitive data exposure and limited injection attacks. First discovered by Nightwatch Cybersecurity researchers on January 19, 2020, the issues were found in the web administration console of the enterprise server management system.

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://threatpost.com/cisco-fixes-high-severity-flaws-in-firepower-security-software-asa/155568/
Impact value: Medium
Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability. A vulnerability in the ARP packet processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Security Appliances could allow an unauthenticated, adjacent attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition on an affected device.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-air-ap-dos
Impact value: Medium
Cisco Aironet Series Access Points Denial of Service Vulnerability. A vulnerability in the internal packet processing of Cisco Aironet Series Access Points (APs) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected AP if the switch interface where the AP is connected has port security configured.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/microsoft/microsofts-family-safety-parental-control-app-opens-for-testing/
Impact value: Informative
Microsoft's Family Safety parental control app opens for testing. Microsoft has announced today that users can signup to preview their Family Safety parental control app on Android and iOS devices. With the Microsoft Family Safety app for Android and iOS, you can get information about your family’s activity including what your kids are doing online across Windows and Xbox devices.

www.ke-cirt.go.ke