NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
13th 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	1	0	2
System Vulnerabilities	2	0	0	0
Malware	0	3	0	0
DDoS/Botnets	0	1	0	0
Spam & Phishing	0	1	1	0
Web Security	1	0	0	2
Updates & Alerts	0	0	0	3

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1 : Threat Post (https://threatpost.com/)

https://threatpost.com/texas-courts-ransomware-attack/155711/

Impact value: Informative

Texas Courts Won't Pay Up in Ransomware Attack. A ransomware attack has hit the information technology office that supports Texas appellate courts and judicial agencies, leading to their websites and computer servers being shut down. The office said that it will not pay the ransom requested by the cybercriminals.

https://threatpost.com/leaked-nhs-docs-roadmap-concerns-contact-tracing-app/155719/

Impact value: High

Leaked NHS Docs Reveal Roadmap, Concerns Around Contact-Tracing App. A COVID-19 contact-tracing app to be rolled out by the UK's National Health Service (NHS) has been thrust into the spotlight thanks to sensitive documents being leaked via a public Google Drive link.

Source 2 : ZDnet (https://www.zdnet.com/)

https://www.zdnet.com/article/us-formally-accuses-china-of-hacking-us-entities-working-on-covid-19-research/

Impact value: Informative

US formally accuses China of hacking US entities working on COVID-19 research. The US government has formally accused China today of orchestrating cyber-attacks against US companies working on COVID-19 research. The accusations were levied in a joint statement issued by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA) and the Federal Bureau of Investigation (FBI). The two agencies said they're investigating attacks carried out by "PRC-affiliated cyber actors and non-traditional collectors."

System vulnerabilities

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/sap-may-2020-security-patch-day-delivers-critical-updates/
Impact value: Critical
SAP May 2020 Security Patch Day delivers critical updates. Enterprise software maker SAP released its May security patches, which cover six critical issues in several of its products, three of them with a severity score very close to maximum. All but one of these flaws are remotely exploitable, require no user interaction, and have a low attack complexity. Not all of them are new vulnerabilities, though; one of them is an update to a security note from April 2018.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/printdemon-vulnerability-impacts-all-windows-versions/
Impact value: Critical
PrintDemon vulnerability impacts all Windows versions. Two security researchers have published today details about a vulnerability in the Windows printing service that they say impacts all Windows versions going back to Windows NT 4, released in 1996. The vulnerability, which they codenamed PrintDemon, is located in Windows Print Spooler, the primary Windows component responsible for managing print operations

Malware

Source 1 : Fire Eye (https://www.fireeye.com/)
https://www.fireeye.com/blog/threat-research/2020/05/analyzing-dark-crystal-rat-backdoor.html?&web_view=true
Impact value: High
Dark Crystal RAT. Researchers have detected a new C# variant of Dark Crystal RAT that uses new anti-analysis techniques. Some of the capabilities of this new variant include recording keystroke, hiding desktop icons, restarting and shutting down the machine, and transferring clipboard contents to the C2 server.

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/ramsay-malware-air-gapped-networks/155695/
Impact value: High
Ramsay Malware Targets Air-Gapped Networks. A cyber-espionage malware has been discovered that's capable of collecting and exfiltrating sensitive documents from within air-gapped networks. The malware, dubbed Ramsay, is still under active development — so far, researchers have found three different samples, with each sample adding new features. However, Ramsay's targeting of air-gapped networks make the toolkit a formidable threat, researchers say.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/ransomware-now-demands-extra-payment-to-delete-stolen-files/
Impact value: High
Ransomware now demands extra payment to delete stolen files. A ransomware family has begun a new tactic of not only demanding a ransom for a decryptor but also demanding a second ransom not to publish files stolen in an attack.

Botnets/DDoS

Source 1 : We Live Security (https://tools.cisco.com/)
https://www.welivesecurity.com/2020/05/11/breaking-news-app-promises-news-brings-ddos-attacks/?&web_view=true
Impact value: High
ESET suffered a DDoS attack. A DDoS attack was launched against the ESET website through a malicious Android app. The incident had occurred in January 2020 and lasted for seven hours. ESET researchers had immediately identified the malicious app and reported it to Google.

Spam & Phishing

Source 2 : Securi (https://blog.sucuri.net/)
https://blog.sucuri.net/2020/05/youtube-account-recovery-phishing.html
Impact value: High
YouTube phishing. Researchers have come across a new phishing scam that targets YouTube creators. The scam is initiated by sending the data collected through a phishing form to a PHP file hosted at a third-party URL through two separate POST requests. The first POST request is sent after the victim submits their credentials on a phishing page. The second POST request redirects the victim from the phishing page to YouTube's Creator Awards' official page.

Source 3 : BBC (https://www.bbc.com/)
https://www.bbc.com/news/technology-52627272?&web_view=true
Impact value: Medium
Scam store. A scam store, called 'MyTechDomestic,' topped Google search results for days. The store featured hard-to-find gadgets that were priced below the normal price. The site accepted payments only via direct bank transfers.

Web Security

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/google-wordpress-plugin-bug-can-be-exploited-for-black-hat-seo/
Impact value: Critical
Google WordPress plugin bug can be exploited for black hat SEO. A critical bug found in Google's official WordPress plugin with 300,000 active installations could allow attackers to gain owner access to targeted sites' Google Search Console. As Wordfence details, the bug is caused by the disclosure of the proxySetupURL within the HTML source code of admin pages, an URL used to connect the Site Kit plugin to the Google Search Console through Google OAuth.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/vmware-to-acquire-kubernetes-security-platform-octarine/
Impact value: Informative
VMware to acquire Kubernetes security platform Octarine. VMware on Wednesday announced its plans to acquire Octarine, a three year-old company that provides a security platform for Kubernetes applications.

Source 3 : The Standard (https://www.standardmedia.co.ke/)
https://www.standardmedia.co.ke/business/article/2001371248/france-to-force-web-giants-to-delete-some-content-within-the-hour
Impact value: Informative
France to force web giants to delete some content within the hour. Social networks and other online content providers will have to remove paedophile and terrorism-related content from their platforms within the hour or face a fine of up to 4 per cent of their global revenue under a French law voted in on Wednesday.

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 : ZDnet (https://www.zdnet.com/)

https://www.zdnet.com/article/securing-linuxs-master-sysadmin-command-sudo/

Impact value: Informative

Securing Linux's master sysadmin command: Sudo. Sudo is one of the most powerful and dangerous tools in the Unix or Linux system administrator's toolbox. With it, an ordinary user can run commands just as if he or she were the superuser or any other user. Now, One Identity, the company behind the utility, has released a new version of sudo, called sudo 1.9, which gives it better auditing, logging, and security than ever before.

https://www.zdnet.com/article/microsoft-adds-initial-support-for-dns-over-https-doh-in-windows-insiders/

Impact value: Informative

Microsoft adds initial support for DNS-over-HTTPS (DoH) in Windows Insiders. Support for the DNS-over-HTTPS protocol has landed this week in Windows Insiders, Microsoft's experimental version of Windows, where the company tests new features before making them broadly available. When activated, this new DoH client will allow the Windows OS to use the DoH protocol instead of classic DNS when connecting to the internet and when resolving web domains.

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

https://www.bleepingcomputer.com/news/microsoft/may-2020-patch-tuesday-microsoft-fixes-111-vulnerabilities-13-critical/

Impact value: Informative

Microsoft to drop support for Windows 10 on 32-bit systems. An update to the Windows 10 Minimum hardware requirements document, Microsoft states that starting with Windows 10 2004, new OEM computers will be required to use 64-bit builds of the operating system.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke