NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
25th 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	0	0	3
System Vulnerabilities	0	2	1	0
Malware	0	0	3	0
DDoS/Botnets	0	0	0	0
Spam & Phishing	0	0	0	0
Web Security	0	0	0	1
Updates & Alerts	0	0	0	1

Top Stories

Source 1 : Time (https://time.com/)
https://time.com/5859079/julian-assange-hackers-anonymous-indictment/
Impact value: Informative

The US Department of Justice has filed today a superseding indictment against WikiLeaks founder Julian Assange. The newly updated indictment clarifies the depth of Assange's alleged crimes by broadening the original charges to include more serious accusations that the WikiLeaks founder conspired and tried to recruit Anonymous and LulzSec hacker to carry out hacking on his behalf.

Source 2 : ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/aws-launches-honeycode-a-no-code-app-building-service/
Impact value: Informative

AWS today announced the beta launch of Amazon Honeycode, a new, fully managed low-code/no-code development tool that aims to make it easy for anybody in a company to build their own applications. All of this, of course, is backed by a database in AWS and a web-based, drag-and-drop interface builder.

Source 3 : The Verge (https://www.theverge.com/)
https://www.theverge.com/2020/6/24/21301470/whatsapp-payments-brazil-suspended-central-bank-risk-regulators
Impact value: Informative

Brazil's central bank and the country's antitrust watchdog Cade have ordered the suspension of financial transactions via WhatsApp as part of an investigation into the threats the app presents to the national payments system.

System vulnerabilities

Source 1 : Microsoft (https://www.microsoft.com/)
https://www.microsoft.com/security/blog/2020/06/24/defending-exchange-servers-under-attack/
Impact value: Medium
Microsoft’s Defender ATP Research Team released guidance on how to defend against attacks targeting Exchange servers with the use of behavior-based detection. Microsoft researchers analyzed multiple campaigns targeting Exchange servers in early April which showed how the malicious actors deploying web shells. The CVE-2020-0688 flaw resides in the Exchange Control Panel (ECP) component, the root cause of the problem is that Exchange servers fail to properly create unique keys at install time. A remote, authenticated attacker could exploit the CVE-2020-0688 vulnerability to execute arbitrary code with SYSTEM privileges on a server and take full control.

Source 2 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/vmware-patches-several-vulnerabilities-allowing-code-execution-hypervisor
Impact value: High
VMware has addressed 10 vulnerabilities affecting ESXi, Workstation and Fusion products, including critical and high-severity issues that can be exploited by attackers to execute arbitrary code on the hypervisor. The most serious issue is a critical use-after-free flaw, tracked as CVE-2020-3962, that affects the SVGA device. An attacker who has local access to a virtual machine with 3D graphics enabled could exploit the flaw to execute arbitrary code on the hypervisor from the VM. The 3D graphics are enabled by default on Workstation and Fusion, but it is not enabled by default on the ESXi product.

System vulnerabilities

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/list-of-ripple20-vulnerability-advisories-patches-and-updates/
Impact value: High
A set of serious network security vulnerabilities collectively known as Ripple20 roiled the IoT landscape when they came to light recently, and the problems they pose for IoT-equipped businesses could be both dangerous and difficult to solve. Ripple20 was originally discovered by Israel-based security company JSOF in September 2019. It affects a lightweight, proprietary TCP/IP library created by a small company in Ohio called Treck, which has issued a patch for the vulnerabilities. Several of those vulnerabilities would allow for remote-code execution, allowing for data theft, malicious takeovers and more, said the security vendor.

Malware

Source 1 : Paloalto Networks (https://unit42.paloaltonetworks.com/)
https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/
Impact value: Medium

A new devilish malware is targeting Windows systems with cryptojacking and DDoS capabilities. Security experts have identified a self-propagating malware, dubbed Lucifer, that targets Windows systems with cryptojacking and distributed denial-of-service (DDoS) attacks. The never-before-seen malware initially tries to infect PCs by bombarding them with exploits in hopes of taking advantage of an "exhaustive" list of unpatched vulnerabilities. While patches for all the critical and high-severity bugs exist, the various companies impacted by the malware had not applied the fixes.

Source 2 : Android Authority (https://www.androidauthority.com/)
https://www.androidauthority.com/covid-19-ransomware-1132190/
Impact value: Medium

The CryCryptor malware strain is a brand-new family of threats, leveraging COVID-19 to spread. A new strain of ransomware has arisen in Canada, targeting Android users and locking up personal photos and videos. Called CryCryptor, it has initially been spotted pretending to be the official COVID-19 tracing app provided by Health Canada. It's propagating via two different bogus websites that pretend to be official, according to ESET researchers – one called tracershield.ca.

Source 3 : Threatpost (https://threatpost.com/)
https://threatpost.com/self-propagating-lucifer-malware-targets-windows-systems/156883/
Impact value: Medium

Security experts have identified a new malware targeting Windows systems with crypto-jacking and DDoS attacks, named Lucifer for its devilish features. Lucifer is a self-propagating malware, and initially bombards PCs in hopes of taking advantage of vulnerabilities. The malware capitalizes on lists of unpatched vulnerabilities to obtain a foothold in their targets' systems.

Web Security

Source 1 : Helpnet Security (https://www.helpnetsecurity.com/)
https://www.helpnetsecurity.com/2020/06/24/microsoft-defender-android-linux/
Impact value: Informative
A few Microsoft Defender Advanced Threat Protection (ATP) enhancements that expand the product's operating system platform support were announced by Microsoft this month. The Microsoft Defender ATP security solution, which works with the Microsoft Defender Security Center portal to protect endpoints and client devices against threats, is now at the general availability (GA) release stage for use with Linux server machines. Microsoft is previewing Microsoft Defender ATP for Android devices.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)

https://www.us-cert.gov/ncas/bulletins/sb20-174

Vulnerability Summary for the Week of June 15, 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 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/nvidia-patches-high-severity-flaws-in-windows-linux-drivers/
Impact value: Informative
Graphics chipmaker Nvidia has fixed two high-severity flaws in its graphics drivers. Attackers can exploit the vulnerabilities to view sensitive data, gain escalated privileges or launch denial-of-service (DoS) attacks in impacted Windows gaming devices. Nvidia’s graphics driver (also known as the GPU Display Driver) for Windows is used in devices targeted to enthusiast gamers; it’s the software component that enables the device’s operating system and programs to use its high-level, gaming-optimized graphics hardware.

www.ke-cirt.go.ke