NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
18th May 2020

COMMUNICATIONS
AUTHORITY OF KENYA

Summary Headlines	Impact Metric Against Count of Events			
	Critical	High	Medium	Informative
Regional Highlights	0	0	0	1
Top Stories	0	0	0	2
System Vulnerabilities	0	2	0	0
Malware	0	1	1	0
DDoS/Botnets	0	0	1	0
Spam & Phishing	0	0	0	1
Web Security	0	0	0	1
Updates & Alerts	0	1	0	1

Regional Highlights

Source 1 : Gadgets Africa (https://gadgets-africa.com/)
https://gadgets-africa.com/2020/05/18/jkuat-students-develop-contact-tracing-app/

Impact value: Informative

Students Victor Muthembwa, Boniface Bundi and Crispus Nyaberi from Jkuat have come up with a ‘Contact Tracing and Case Management App’ which will help to identify who, where and when a person gets into contact with a Covid-19 positive individual. The app as an important asset in the fight against Covid-19 since it is digital and specifically focuses on tracing contacts who use public transport. The innovators have already partnered with Super Metro Bus Sacco, which ply the Nairobi-Thika route, as well as Kikuyu and Uthiru areas where the concept is working successfully.

Top Stories

Source 1 : ZDNet (https://www.zdnet.com/)

https://www.zdnet.com/article/illinois-blames-glitch-for-exposure-of-applicant-social-security-numbers-private-data/

Impact value: Informative

Government officials said that a glitch in the State of Illinois’ Pandemic Unemployment Assistance (PUA) program exposed thousands of people’s Social Security Numbers (SSNs) and other private data. Jordan Abudayyeh, a spokesperson for Illinois Governor J. B. Pritzer, sent a statement to WBEZ on May 16. In it, she revealed that the Illinois Department of Employment Security (IDES) had learned of a security incident involving its PUA program.

https://www.zdnet.com/article/fbi-criticizes-apple-for-not-helping-crack-pensacola-shooters-iphones/

Impact value: Informative

Federal law enforcement officials said Monday they had unlocked the iPhones of the perpetrator of a December terrorist attack at a U.S. Naval base — and sharply criticizing Apple for not granting them access to those encrypted communications. FBI technicians cracked the phones of a Saudi aviation student who killed three U.S. sailors at the Naval Air Station Pensacola, uncovering evidence linking him to an Al Qaeda affiliate, Attorney General William Barr said. Barr and FBI Director Christopher Wray urged Silicon Valley companies to write software that allows investigators to access encrypted communications with a warrant, a move that technology firms and security experts have criticized for years.

System vulnerabilities

Source 1 : Forbes (https://www.forbes.com/)
https://www.forbes.com/sites/zakdoffman/2020/05/17/microsoft-confirms-serious-new-windows-10-security-problem-says-go-buy-a-new-pc/#6d5cf83a4347

Impact value: High

Microsoft has confirmed a newly reported security vulnerability called “Thunderspy” that lies within a vulnerability in its THunderbolt ports. The vulnerability enables an attacker with physical PC access to adjust or change the port’s controller firmware, effectively disabling its security and presenting huge risks for the victim. Last week, consumers were informed that almost all Windows PCs with Thunderbolt ports are vulnerable to the attack.

Source 2 : Claroty (https://blog.claroty.com/)
https://blog.claroty.com/software-based-plc-vulnerabilities-enable-remote-code-execution

Impact value: High

Vulnerabilities discovered by a researcher at industrial cybersecurity firm Claroty in Opto 22’s SoftPAC virtual programmable automation controller (PAC) expose operational technology (OT) networks to attacks. SoftPAC is a software-based automation controller that can be hosted on a Windows device, which, according to the vendor, makes it particularly useful for applications that require more file storage, computing power, or frequent access to files.

Malware

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

https://www.bleepingcomputer.com/news/security/fbi-warns-of-prolock-ransomware-decryptor-not-working-properly/

Impact value: Medium

The FBI has issued an alert warning the public that the ProLock ransomware decryptor does not work to secure data in the event of a ransomware attack. Earlier this month, the FBI released a flash alert informing organizations of the new threat actor, stating that it targets US healthcare, government, financial, and retail entities. With the ProLock ransomware, files larger than 64MB will likely be corrupted during the decryption process.

Source 2 : Security Affairs (https://securityaffairs.co/)

https://securityaffairs.co/wordpress/103395/malware/mandrake-android-platform.html

Impact value: High

Security researchers from Bitdefender have just released details of a highly sophisticated attack which can enable hackers to take control of a device without the owner ever knowing. Named "Mandrake", the spyware campaign is thought to have been targeting Android users for the past four years. Unlike most attacks, which spam millions of devices by infiltrating the Play Store and tricking users into downloading the dodgy apps, this latest threat is much smarter and far more sinister.

Botnets/DDoS

Source 1 : Paloalto (https://unit42.paloaltonetworks.com/)
https://unit42.paloaltonetworks.com/hoaxcalls-mirai-target-legacy-symantec-web-gateways/

Impact value: Medium

Cyberattackers are targeting a post-authentication remote code-execution vulnerability in Symantec Secure Web Gateways as part of new Mirai and Hoaxcalls botnet attacks. Hoaxcalls first emerged in late March, as a variant of the Gafgyt/Bashlite family; it’s named after the domain used to host its malware, Hoaxcalls.pw.

Spam & Phishing

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/new-microsoft-365-sign-in-pages-already-spoofed-for-phishing/

Impact value: Informative

Microsoft’s newly updated sign-in pages have already been succumbed to phishing campaigns by attackers. The new sign-in page update was created in an attempt to lower the bandwidth requirements of the pre-existing Azure AD sign-in pages. Additionally, it allowed Microsoft users to more easily determine if they were the potential victims of outdated phishing tools. The Azure AD sign-in experience was updated at the end of February and released to consumers the first week in April, yet attackers have found ways to spoof these new pages.

Web Security

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

https://www.bleepingcomputer.com/news/google/google-chrome-to-tidy-up-tabs-with-tab-groups-collapse-feature/

Impact value: Informative

The rollout of tabbed grouping in Google Chrome is something that aims to address the problem of working with large numbers of tab at once. The new feature makes it possible to group related tabs together and treat them as a single entity for ease of navigation and management. But Google is not stopping there. The company is already in the process of upgrading the feature with new options; collapsible tab groups are now available to test in the Canary build of Chrome 85.

Bulletins

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

https://www.us-cert.gov/ncas/bulletins/sb20-139

Vulnerability Summary for the Week of May 11, 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/microsoft/microsoft-edge-canary-now-lets-you-read-aloud-your-pdf-files/

Impact value: Informative

Microsoft has been working on improving the read aloud feature for some time now and the company has now added support for Read Aloud for PDFs. The feature was available in the Legacy Edge and has been carried forward to Chromium-based Edge. Read Aloud is currently hidden behind a flag but if you're interested in trying out the feature then you can do so

Source 2 : Cisco (https://tools.cisco.com/security/center/publicationListing.x)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-fpsnort

Impact value: High

A vulnerability in the Secure Sockets Layer (SSL) packet reassembly functionality of the detection engine in Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause the detection engine to consume excessive system memory on an affected device, which could cause a denial of service (DoS) condition. Cisco has released software updates that address this vulnerability.

www.ke-cirt.go.ke