NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
15th 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	1	2	0	1
System Vulnerabilities	1	1	0	1
Malware	0	1	0	1
DDoS/Botnets	0	0	0	1
Spam & Phishing	0	2	0	0
Web Security	0	1	0	1
Updates & Alerts	0	0	2	1

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

Source 1 : ISBuzz News (https://www.informationsecuritybuzz.com/)
https://www.informationsecuritybuzz.com/expert-comments/experts-reaction-on-accessories-giant-claires-hacked-to-steal-credit-card-info/
Impact value: High
Claire's breached. The U.S.-based jewelry and accessory giant Claire's and its subsidiary Icing were compromised in April in a Magecart attack. This enabled the attackers to steal customers' credit card details. The skimmer was served from a domain that looked similar to that of the company's legitimate domain.

Source 2 : Helpnet Security (https://www.helpnetsecurity.com/)
https://www.helpnetsecurity.com/2020/06/15/magecart-claires-intersport/?web_view=true
Impact value: High
Intersport also attacked. Intersport's web store had suffered a Magecart-like attack after crooks planted skimmer code on the checkout page to steal credit card details. The incident had occurred on April 30 and May 14, 2020.

Source 3 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/south-african-bank-to-replace-12m-cards-after-employees-stole-master-key/?&web_view=true
Impact value: Critical
South African bank to replace 12m cards after employees stole master key. Postbank, the banking division of South Africa's Post Office, has lost more than $3.2 million from fraudulent transactions and will now have to replace more than 12 million cards for its customers after employees printed and then stole its master key. The Sunday Times of South Africa, the local news outlet that broke the story, said the incident took place in December 2018 when someone printed the bank's master key on a piece of paper at its old data center in the city of Pretoria.

System vulnerabilities

Source : Security Week (https://www.securityweek.com/)

https://www.securityweek.com/gtp-vulnerabilities-expose-4g5g-networks-high-impact-attacks

Impact value: High

GTP vulnerabilities. Vulnerabilities in the GPRS Tunneling Protocol (GTP) can expose 4G and 5G cellular networks to a variety of attacks. This includes denial of service attacks, impersonation attacks, and identity fraud. The flaws impact both mobile operators and their clients.

https://www.securityweek.com/new-eavesdropping-technique-relies-light-bulb-vibrations

Impact value: Informative

Lamphone attack. A group of researchers has devised a new side-channel attack technique, called Lamphone, for eavesdropping on conversations. It relies on the fluctuations in air pressure on the surface of a hanging bulb. The researchers have successfully tested the technique by targeting an office room located on the third floor of an office building.

https://www.securityweek.com/critical-vulnerabilities-expose-siemens-logo-controllers-attacks?&web_view=true

Impact value: Critical

Critical Vulnerabilities Expose Siemens LOGO! Controllers to Attacks. According to Siemens, the vulnerabilities impact all versions of its LOGO!8 BM devices, which are designed for basic control tasks. SIPLUS versions, which are meant for use in extreme conditions, are also affected. The German industrial giant has yet to release patches for the vulnerabilities, which have been described as missing authentication issues, but it has told customers that they can reduce the risk of exploitation by applying defense-in-depth measures.

Malware

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/us-bank-customers-targeted-in-ongoing-qbot-campaign/

Impact value: High

US bank customers targeted in ongoing Qbot campaign. Security researchers at F5 Labs have spotted ongoing attacks using Qbot malware payloads to steal credentials from customers of dozens of US financial institutions. Qbot (also known as Qakbot, Pinkslipbot, and Quakbot) is a banking trojan with worm features used to steal banking credentials and financial data, as well as to log user keystrokes, deploy backdoors, and drop additional malware on compromised machines.

Source 2 : Check Point (https://blog.checkpoint.com/)
https://blog.checkpoint.com/2020/06/15/mays-most-wanted-malware-ursnif-banking-trojan-ranks-on-top-10-malware-list-for-first-time-over-doubling-its-impact-on-organizations/?web_view=true

Impact value: Informative

Ursnif Banking Trojan Ranks On Top 10 Malware List for First Time, Over Doubling Its Impact On Organizations. The latest Check Point Global Threat Index for May 2020 has found several malicious spam campaigns distributing the Ursnif banking trojan, which caused it to jump up 19 places to 5th in the Top Malware list, doubling its impact on organizations worldwide. Check Point researcher's warn that with the Dridex, Agent Tesla and Ursnif banking trojans all ranking in the malware top 5 in May, it is clear cyber criminals are focusing on using malware that enables them to monetize their victim's data and credentials.

Botnets/DDoS

Source : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/fraudster-gets-maximum-jail-time-for-news-site-ddos-extortion/

Impact value: Informative

Fraudster gets maximum jail time for news site DDoS extortion. Iranian-born U.S. citizen Andrew Rakhshan, previously convicted in Canada for fraud, was sentenced to the maximum sentence of five years and ordered to pay over $500,000 after being found guilty of launching several distributed denial of service (DDoS) attacks against news websites.

Spam & Phishing

https://www.bleepingcomputer.com/news/security/attackers-impersonate-secure-messaging-site-to-steal-bitcoins/?&web_view=true

Impact value: High

Cybersquatting. Cybercriminals have reportedly created a legitimate-looking copy of privnote.com to trick users by manipulating their text content. This enabled the crooks to steal bitcoin by changing wallet addresses contained in requests sent via the platform.

https://www.bleepingcomputer.com/news/security/extortionists-threaten-to-destroy-sites-in-fake-ransom-attacks/?&web_view=true

Impact value: High

Spamdexing. Scammers are using blackhat SEO techniques to threaten website owners into paying ransoms between $15,00 and $3,000 in bitcoins. The fraudsters make a fake claim that they have exfiltrated their databases and will leak the same on the internet unless a ransom is paid.

Web Security

Source 1 : The Hackers News (https://thehackernews.com/)
https://thehackernews.com/2020/06/webauthn-passwordless.html
Impact value: Informative
WebAuthn Passwordless Authentication Now Available for Atlassian Products. WebAuthn is a browser-based security standard recommended by World Wide Web Consortium (W3C) that allows web apps to simplify and safeguard user authentication by utilizing registered devices as factors. It relies on public-key cryptography to prevent sophisticated phishing attacks. WebAuthn is part of the FIDO2 framework - various technologies that permit passwordless authentication among web browsers, servers, and authenticators.
This security standard is supported by Windows 10 and Android platforms and browsers such as Chrome, Edge, Safari, and Firefox.

Source 2 : Bank Info Security (https://www.bankinfosecurity.com/)
https://www.bankinfosecurity.com/delivery-hero-confirms-foodora-data-breach-a-14435?&web_view=true
Impact value: High
Delivery Hero Confirms Foodora Data Breach. Delivery Hero, the online food delivery service, has confirmed a data breach of its Foodora brand. Breached information from 14 countries includes personal details for 727,000 accounts - names, addresses, phone numbers and hashed passwords. It also contains latitude and longitude coordinates to six decimal points, which is accurate to within just a few inches. No financial data was leaked.

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/security/intel-adds-cpu-level-malware-protection-to-tiger-lake-processors/
Impact value: Informative
Intel adds CPU-level malware protection to Tiger Lake processors. Intel has announced a new CPU-level security capability that offers protection against malware using control-flow hijacking attack methods. Termed as Control-Flow Enforcement Technology (Intel CET), the software will guard devices that will use the upcoming Tiger Lake mobile processors. It includes two new capabilities- Shadow Stack and Indirect Branch Tracking (IBT).

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke