NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES

16th 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	3	0	0
System Vulnerabilities	0	3	0	0
Malware	0	3	0	0
DDoS/Botnets	0	0	0	1
Spam & Phishing	0	1	1	0
Web Security	0	2	0	0
Updates & Alerts	2	0	1	0

Top Stories

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/google-alerts-catches-fake-data-breach-notes-pushing-malware/
Impact value: High
Google Alerts catches fake data breach notes pushing malware. Fraudsters recently have started to push fake data breach notifications for big company names to distribute malware and scams. They're mixing black SEO, Google Sites, and spam pages to direct users to dangerous locations.

Source 2 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/super-secretive-russian-disinfo-operation-discovered-dating-back-to-2014/
Impact value: High
Super secretive Russian disinfo operation discovered dating back to 2014. Researchers uncover six-years-worth of Russian attempts to mold international politics using fake news and forged documents. Social media research group Graphika published today a 120-page report [PDF] unmasking a new Russian information operation of which very little has been known so far.

Source 2 : Cyber Scoop (https://www.cyberscoop.com/)
https://www.cyberscoop.com/vendetta-taiwan-coronavirus-telefonica/
Impact value: High
'Vendetta' hackers are posing as Taiwan's CDC in data-theft campaign. A mysterious hacking group has been posing as Taiwan's top infection-disease official in an attempt to steal sensitive data from Taiwanese users, researchers said Monday. The hackers sent meticulously written spearphishing emails to a select group of targets, which may have included Taiwan's Centers for Disease Control employees, according to ElevenPaths, the cybersecurity unit of Spanish telecommunications firm Telefónica Group, which uncovered the activity.

System vulnerabilities

Source 1 : JSOFT (https://www.jsof-tech.com/)
https://www.jsof-tech.com/ripple20/
Impact value: High

Ripple20 vulnerability. A total of 19 vulnerabilities, collectively known as Ripple20, have been found affecting millions of IoT devices. The flaws exist in the low-level TCP/IP software library developed by Treck Inc. They can be exploited to take control of devices and steal data from infected ones. Some of the affected vendors include HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, and Baxter.

Source 2 : We live Security (https://www.welivesecurity.com/)
https://www.welivesecurity.com/2020/06/15/warning-issued-hackable-security-cameras/
Impact value: High

Hackable security cameras. Wireless security cameras manufactured by Alptop, Besdersec, COOAU, CPVAN, Ctronics, Dericam, Jennov, LEFTEK, Luowice, and QZT are affected by serious vulnerabilities that can expose users' data to attackers. These vulnerabilities, which are tracked as CVE-2019-11219 and CVE-2019-11220, exist in the P2P feature of the CamHi app that is used by the cameras.

Source 3 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/oracle-ebs-vulnerabilities-allow-hackers-tamper-financial-records
Impact value: Critical

Oracle fixes two flaws. Oracle has patched two vulnerabilities found in its E-Business Suite solution. The flaws, tracked as CVE-2020-2586 and CVE-2020-2587, can allow attackers to take control of the EBS environment. The flaws can also enable unauthorized hackers to alter financial data held in the solution.

Malware

Source 1 : Gdata (https://www.gdatasoftware.com/)
https://www.gdatasoftware.com/blog/strrat-crimson
Impact value: High
STRRAT malware. A newly discovered Java-based STRRAT malware includes a ransomware module apart from information-stealing capabilities. Telemetry shows that the malware has infected many users in Germany. It is distributed via spam emails that include a malicious attachment named “NEW ORDER.jar”.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/draftkings-discloses-sbtech-ransomware-attack-in-sec-filing/
Impact value: High
DraftKings discloses SBTech ransomware attack in SEC filing. In a Form S-1 registration statement filed with the SEC as required to go public on the Nasdaq stock market, DraftKings disclosed that SBTech suffered a ransomware attack on March 27th, right before the merger finalized. This outage also caused online betting sites that utilized SBTech's platform to go down.

Source 2 : ZDnet (https://www.zdnet.com/)
https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/?web_view=true
Impact value: High
Citizen Lab and Amnesty International Uncover Spyware Operation Against Indian Human Rights Defenders. The targeting in this campaign occurred between January and October 2019. Targets were sent emails disguised as important communications, such as official summonses, bearing links to malicious software disguised as important documents. If opened, targets’ computers would have been infected with NetWire, a piece of commodity malware.

Botnets/DDoS

Source 1 : 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

Source 2 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/nhs-100-email-accounts-hijacked/
Impact value: High

NHS's phishing campaign. The NHS disclosed that 113 email accounts were compromised and used to send malicious spam outside the health service between May 30, and June 1, 2020. The subject lines of these emails either included the recipient's names or were left blank. Furthermore, these emails contained a link to a fake log-in page featuring the NHS logo. Following the incident, NHS changed the passwords of the compromised accounts.

Source 3 : Fortinet (https://www.fortinet.com/)
https://www.fortinet.com/blog/threat-research/global-malicious-spam-campaign-using-black-lives-matter
Impact value: Medium

TrickBot Trojan. Several spam campaigns around 'Black Lives Matter' have been detected by security researchers. The campaigns are executed using phishing emails that have a variety of subject lines and an attached malicious Microsoft Word document. These documents work as a delivery channel for malware like TrickBot trojan. The campaign is spread across Canada, the United States, France, and Cyprus.

Web Security

Source 1 : SC Magazine (https://www.scmagazine.com/)
https://www.scmagazine.com/website-web-server-security/anonymous-claims-credit-for-taking-down-atlanta-pd-website/?web_view=true
Impact value: High
Anonymous' claims credit for taking down Atlanta PD website. An apparent tweet from the Anonymous hacking group is claiming credit for perpetrating a cyberattack on the Atlanta police department web site, stating that the act was retaliation for the June 12 fatal police shooting of Rayshard Brooks. "Atlanta police officers involved in fatal shooting of Rayshard Brooks. @Atlanta_Police has been taken #Offline" states a tweet from Anonymous USA (@AnonOpUSA) that was posted at 8:24 a.m. on June 14.

Source 2 : Financial Review (https://www.afr.com/)
https://www.afr.com/technology/hacked-aussie-websites-for-sale-on-dark-web-20200612-p55227?&web_view=true
Impact value: High
Aussie websites for sale on dark web. ASX-listed companies, financial services firms, law firms, an insurance company and an adult entertainment store are among hundreds of Australian websites for sale on the dark web. The websites are part of a list of 43,000 hacked servers available for sale on MagBo, the shadowy online marketplace where cyber criminals sell access to websites for as little as $US1 ($1.46) and as much as $US10,000.

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 : Dark Reading (https://www.darkreading.com/)
https://www.darkreading.com/vulnerabilities---threats/microsoft-releases-update-for-dos-flaw-in-net-core-/d/d-id/1338089?&web_view=true
Impact value: Medium
Microsoft Releases Update for DoS Flaw in .NET Core. Last week Microsoft published a revision to CVE-2020-1108, a denial-of-service (DoS) vulnerability in the .NET Core and .NET Framework. To fully address the flaw, the company released updates for PowerShell Core 6.2 and PowerShell 7.0, according to an email advisory sent on June 11.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/vlc-media-player-3011-fixes-severe-remote-code-execution-flaw/
Impact value: Critical
VLC Media Player 3.0.11 fixes severe remote code execution flaw. VideoLan has released VLC Media Player 3.0.11, and it is now available for Windows, Mac, and Linux. In addition to bug fixes and improvements, this release also fixes a security vulnerability that could allow attackers to remotely execute commands or crash VLC on a vulnerable computer. This vulnerability is tracked as CVE-2020-13428 and is a "buffer overflow in VLC's H26X packetizer" that would allow attackers to execute commands under the same security level as the user if properly exploited.

https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-flaws-in-illustrator-after-effects-more/
Impact value: Critical
Adobe fixes critical flaws in Illustrator, After Effects, more. Adobe has released out-of-band security updates to address 18 critical flaws that could allow attackers to execute arbitrary code on systems running vulnerable versions of Adobe After Effects, Illustrator, Premiere Pro, Premiere Rush, and Audition on Windows and macOS devices.

www.ke-cirt.go.ke