NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
10th 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	1	2	0	0
Malware	0	2	1	0
DDoS/Botnets	0	1	0	0
Spam & Phishing	0	2	0	0
Web Security	0	2	0	0
Updates & Alerts	0	0	2	1

Top Stories

Source 1 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/nintendo-says-300000-accounts-breached-after-hack
Impact value: High
Nintendo's accounts affected. The Japanese gaming giant, Nintendo, has disclosed a data breach that affected around 300,000 accounts. The hack, which took place in early April, impacted the birth dates and email addresses of gamers. However, no credit card details were compromised in the incident.

Source 2 : Malwarebytes (https://blog.malwarebytes.com/)
https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/
Impact value: High
Edesur S.A attacked. In addition to Honda Motor Co., the Snake ransomware has also infected Edesur S.A, one of the companies belonging to Enel Argentina. Reports suggest that both the companies were hacked through systems with publicly exposed Remote Desktop Protocol (RDP) ports.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/self-destructing-skimmer-steals-credit-cards-of-greenworks-customers/
Impact value: High
Another MageCart attack. The GreenWorks website got compromised by a highly sophisticated self-cleaning and self-destructing skimmer designed to steal payment card details of users. It is found that the card details stolen from the website are redirected to a server at congolo[.]pro controlled by hackers.

System vulnerabilities

Source 1 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/critical-remote-code-execution-vulnerabilities-patched-ibm-websphere
Impact value: Critical
IBM patches flaws. IBM has patched two critical vulnerabilities affecting its WebSphere Application Server product. These flaws could be exploited by unauthenticated attackers to execute arbitrary code with elevated privileges.

Source 2 : Talos (https://blog.talosintelligence.com/)
https://blog.talosintelligence.com/2020/06/vuln-spotlight-siemens-logo-june-2020.html?&web_view=true
Impact value: High
Flawed Siemens LOGO!PLC patched. A flaw found in the Siemens LOGO! PLC models have been patched recently. The security issue, tracked as CVE-2020-7589, could allow an adversary to carry out a variety of malicious activities.

Source 3 : The Register (https://www.theregister.com/)
https://www.theregister.com/2020/06/10/gnutls_patches_security_hole/?&web_view=true
Impact value: High
GnuTLS patches security holes. A two-year-old bug that was lurking in the GnuTLS servers has been fixed last week. The bug could make TLS 1.3 sessions vulnerable to attacks.

Malware

Source 1 : White Ops (https://www.whiteops.com/)
https://www.whiteops.com/blog/beauty-and-the-fraud-beast
Impact value: High
Malicious apps. Around 38 malicious Android apps with more than 20 million downloads were removed from the Google Play Store for conducting ad fraud. Some of these apps are 'Rose Photo Editor & Selfie Beauty Camera' and 'Pinut Selfie Beauty Camera & Photo Editor.'

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/thanos-ransomware-auto-spreads-to-windows-devices-evades-security/
Impact value: High
Thanos ransomware auto-spreads to Windows devices, evades security. The Thanos ransomware is the first to use a researcher-disclosed RIPlace anti-ransomware evasion technique as well as numerous other advanced features that make it a serious threat to keep an eye on. Thanos first began private distribution at the end of October 2019, but it was not until January 2020 when victims seeking help for what was called then the Quimera Ransomware.

Source 3 : Threat Post (https://threatpost.com/)
https://threatpost.com/legitimate-italian-guloader-obfuscator/156443/
Impact value: Medium
Encryption Utility Firm Accused of Bundling Malware Functions in Product. An Italian company that sells what it describes as a legitimate encryption utility is being used as malware packer for the cloud-delivered malicious GuLoader dropper, claim researchers. The tool, according a recent investigation, creates GuLoader samples and helps the malware avoid antivirus detection.

Botnets/DDoS

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/kingminer-botnet-brute-forces-mssql-databases-to-install-cryptocurrency-miner/
Impact value: High

KingMiner botnet returns. Security researchers have detected a new KingMiner botnet operation that targets MSSQL databases with brute-force attacks. Once hackers break into a vulnerable MSSQL system, they create another database user named ‘dbhelp’ and install a cryptocurrency miner that abuses the server’s resources to generate profits for the gang.

Spam
&
Phishing

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/fake-spacex-youtube-channels-scam-viewers-out-of-150k-in-bitcoin/
Impact value: High

Giveaway scam. Scammers have hijacked three YouTube channels - ‘Juice TV, Right Human and MaximSakulevich’ - and renamed them to either ‘SpaceX Live’ or ‘SpaceX’ in order to conduct free cryptocurrency giveaway scams. So far, these scams have raked in close to $150,000 in bitcoins. One of these channels has 230,000 subscribers and the other one has 131,000 subscribers. All of these hijacked channels work by live-streaming the previous interviews of Elon Musk or SpaceX conferences while promoting scams that ask viewers to send in a small amount of bitcoin to receive a fake bitcoin giveaway.

Source 3 : The Hill (https://thehill.com/)
https://thehill.com/policy/cybersecurity/501936-senior-official-estimates-30-billion-in-stimulus-funds-will-be-stolen?&web_view=true
Impact value: High

Senior official estimates $30 billion in stimulus funds will be stolen through coronavirus scams. A top official with the U.S. Secret Service said Tuesday that coronavirus-related fraud could lead to $30 billion in federal relief funds being stolen by criminals.

Web Security

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

https://www.bleepingcomputer.com/news/security/self-destructing-skimmer-steals-credit-cards-of-greenworks-customers/

Impact value: High

Another MageCart attack. The GreenWorks website got compromised by a highly sophisticated self-cleaning and self-destructing skimmer designed to steal payment card details of users. It is found that the card details stolen from the website are redirected to a server at congolo[.]pro controlled by hackers.

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

https://www.zdnet.com/article/slovak-police-seize-wiretapping-devices-connected-to-government-network/

Impact value: High

Slovak police seize wiretapping devices connected to government network. Slovak authorities have arrested four suspects on Tuesday as part of an investigation into a series of suspicious devices found connected to the government's official IT network. According to local news site Aktuality, the equipment is believed to have been used for wiretapping purposes and would have allowed threat actors to intercept both internet and telephony operations

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/new-windows-10-smbv3-flaw-can-be-used-for-data-theft-rce-attacks/

Impact value: Informative

New Windows 10 SMBv3 flaw can be used for data theft, RCE attacks. The security flaw, tracked as CVE-2020-1206 and named SMBleed by security researchers at cybersecurity startup ZecOps who found it, was discovered in the same function behind SMBGhost, a pre-auth remote code execution (RCE) vulnerability tagged as "wormable" by Microsoft and patched in March.

www.ke-cirt.go.ke