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

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

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

https://www.zdnet.com/article/solarwinds-hackers-accessed-microsoft-source-code/

Impact value: High

SolarWinds hackers accessed Microsoft source code. The hackers behind the SolarWinds supply chain attack managed to escalate access inside Microsoft's internal network and gain access to a small number of internal accounts, which they used to access Microsoft source code repositories, the company said on Thursday. The OS maker said the hackers did not make any changes to the repositories they accessed because the compromised accounts only had permission to view the code but not alter it. The news comes as an update to the company's internal investigation into the SolarWinds incident, posted today on its blog.

Source 2 : The Hackers News (https://thehackernews.com/)

https://thehackernews.com/2021/01/ticketmaster-to-pay-10-million-fine-for.html

Impact value: Informative

Ticketmaster To Pay $10 Million Fine For Hacking A Rival Company. Ticketmaster has agreed to pay a $10 million fine after being charged with illegally accessing computer systems of a competitor repeatedly between 2013 and 2015 in an attempt to "cut [the company] off at the knees.“ A subsidiary of Live Nation, the California-based ticket sales and distribution company used the stolen information to gain an advantage over CrowdSurge — which merged with Songkick in 2015 and later acquired by Warner Music Group (WMG) in 2017 — by hiring a former employee to break into its tools and gain insight into the firm's operations.

System vulnerabilities

Source : The Hacker News (https://thehackernews.com//)
https://thehackernews.com/2021/01/secret-backdoor-account-found-in.html
Impact value: High
Secret Backdoor Account Found in Several Zyxel Firewall, VPN Products. Zyxel has released a patch to address a critical vulnerability in its firmware concerning a hardcoded, undocumented secret account that could be abused by an attacker to login with administrative privileges and compromise its networking devices. The flaw, tracked as CVE-2020-29583 (CVSS score 7.8), affects version 4.60 present in a wide-range of Zyxel devices, including Unified Security Gateway (USG), USG FLEX, ATP, and VPN firewall products.

Malware

Source 1 : Cyware (https://cyware.com//)

https://cyware.com/news/a-credential-stealer-written-in-autohotkey-scripting-language-8d53e5e8

Impact value: High

A Credential Stealer Written in AutoHotkey Scripting Language. A new credential stealer has been identified that is written in AutoHotkey (AHK) scripting language. In an ongoing attack campaign that started in early 2020, threat actors were found to be distributing this infostealer, focusing on customers of financial organizations located in the U.S. and Canada. The infostealer specifically focuses on credential exfiltration and has targeted multiple banks, such as Royal Bank of Canada, Scotiabank, HSBC, Alterna Bank, EQ Bank, Capital One, Manulife, and ICICI Bank.

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

https://securityaffairs.co/wordpress/112882/hacking/facebook-phishing-campaign-2.html?web_view=true

Impact value: High

Facebook ads used to steal 615000+ credentials in a phishing campaign. Researchers from security firm ThreatNix spotted a new large-scale campaign abusing Facebook ads. Threat actors are using Facebook ads to redirect users to Github accounts hosting phishing pages used to steal victims' login credentials. The campaign targeted more than 615,000 users in multiple countries including Egypt, the Philippines, Pakistan, and Nepal. The landing pages are phishing pages that impersonate legitimate companies. Once the victims provided the credentials, they will be sent to the attackers through a Firestore database and a domain hosted on GoDaddy.

Botnets/DDoS

Source 1 : The Hackers News (https://thehackernews.com/)
https://thehackernews.com/2020/12/citrix-adc-ddos-attack.html
Impact value: High
Attackers Abusing Citrix NetScaler Devices to Launch Amplified DDoS Attacks. Citrix has issued an emergency advisory warning its customers of a security issue affecting its NetScaler application delivery controller (ADC) devices that attackers are abusing to launch amplified distributed denial-of-service (DDoS) attacks against several targets. "An attacker or bots can overwhelm the Citrix ADC [Datagram Transport Layer Security] network throughput, potentially leading to outbound bandwidth exhaustion," the company noted. "The effect of this attack appears to be more prominent on connections with limited bandwidth."

Spam & Phishing

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/beware-paypal-phishing-texts-state-your-account-is-limited/
Impact value: High
Beware: PayPal phishing texts state your account is 'limited'. A PayPal text message phishing campaign is underway that attempts to steal your account credentials and other sensitive information that can be used for identity theft. When PayPal detects suspicious or fraudulent activity on an account, the account will have its status set to "limited," which will put temporary restrictions on withdrawing, sending, or receiving money. The SMS text phishing (smishing) campaign pretends to be from PayPal, stating that your account has been permanently limited unless you verify your account by clicking on a link. "PayPal: We've permanently limited your account, please click link below to verify," the smishing text message reads.

Web Security

Source : Cyware (https://cyware.com//)

https://cyware.com/news/magecart-active-again-with-new-multi-platform-skimmer-95273e1a

Impact value: High

Magecart Active Again with New Multi-platform Skimmer. A multi-platform credit card skimmer has been identified that targets online stores based on popular platforms, including Shopify, Zencart, Woocommerce, and BigCommerce. The skimmer can be used to harvest payment details on compromised stores and is linked to the Magecart group. The first programmatically generated exfiltration domain used by the skimmer in this campaign was first registered on August 31. This suggests that this Magecart campaign has been active for a long time.

https://cyware.com/news/a-security-flaw-could-lead-to-cross-layer-and-dns-poisoning-attacks-850731ef

Impact value: High

A Security Flaw could Lead to Cross-layer and DNS Poisoning Attacks. A new attack technique called cross-layer attack has been identified, which combines vulnerabilities across multiple network protocol layers to attack the target system. It is estimated that one in every 20 web servers could be vulnerable to a security flaw that exists in the Linux kernel, allowing hackers to perform cross-layer attacks. The cross-layer attack is possible because the IPv6 flow label generation algorithm, UDP source port generation algorithm, and the IPv4 ID generation algorithm use the same Pseudo-Random Number Generator (PRNG).

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://us-cert.cisa.gov/ncas/bulletins/sb20-307
Vulnerability Summary for the Week of October 26, 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/cpuoct2020.html
Oracle Critical Patch Update Advisory - October 2020. Advised action to run available security updates.

https://www.oracle.com/security-alerts/alert-cve-2020-14750.html
Oracle WebLogic Server remote code execution vulnerability . This vulnerability is related to CVE-2020-14882, which was addressed in the October 2020 Critical Patch Update.

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/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-voip-phone-flood-dos-YnU9EXOv

Impact value: High

Cisco IP Phone TCP Packet Flood Denial of Service Vulnerability. The vulnerability is due to insufficient TCP ingress packet rate limiting. An attacker could exploit this vulnerability by sending a high and sustained rate of crafted TCP traffic to the targeted device. A successful exploit could allow the attacker to impact operations of the phone or cause the phone to reload, leading to a denial of service (DoS) condition.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)

https://www.bleepingcomputer.com/news/security/google-chrome-fixes-antivirus-file-locking-bug-on-windows-10/

Impact value: Informative

Google Chrome fixes antivirus 'file locking' bug on Windows 10. Google Chrome has fixed a bug that enabled antivirus programs on Windows 10 to lock newly created files. The patching of the bug means antivirus programs running on Windows would no longer block new files generated by the Chrome web browser, such as bookmarks. As a safety precaution, oftentimes antivirus programs temporarily lock newly generated files on a system until these can be scanned and ruled out for malicious activity. On Windows 10 machines, in particular, this created issues for the Google Chrome web browser when it would use `ImportantFileWriter` to output certain files.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke