NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES 5TH 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	3	0	0
System Vulnerabilities	0	2	0	0
Malware	0	2	0	0
DDoS/Botnets	0	0	0	1
Spam & Phishing	0	1	0	0
Web Security	0	1	0	1
Updates & Alerts	0	1	0	1

Top Stories

Source 1 : Cyber News (https://cybernews.com/)
https://cybernews.com/security/after-refusing-to-pay-ransom-us-based-auto-parts-distributor-has-sensitive-data-leaked-by-cybercriminals/
Impact value: High
NameSouth's data leaked. Around 3GB archive of data belonging to US-based auto parts shop NameSouth has been publicly leaked following a failed ransom negotiation. Claimed to be an act of the NetWalker ransomware group, the leaked data includes confidential company data such as financial and accounting data, credit card statements, and various legal documents.

Source 2 : Ciso Mag (https://cisomag.eccouncil.org/)
https://cisomag.eccouncil.org/juspay-data-breach/
Impact value: High
JusPay data breach. India-based payments startup Juspay has confirmed a data breach that affected the credit and debit card details of 35 million users. According to researchers, the card data is up for sale on the dark web. The firm is a payment partner for many Indian online platforms such as Amazon, Swiggy, and Makemytrip.

Source 3 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/hacker-posts-data-of-10-000-american-express-accounts-for-free/
Impact value: High
Hacker posts data of 10,000 American Express accounts for free. A threat actor has posted data of 10,000 American Express credit card holders on a hacker forum for free. As analyzed by BleepingComputer, the leaked sample data set of 10,000 records exposes full American Express account (credit card) numbers and customers' personally identifiable information (PII) including name, full address, phone numbers, date of birth, gender, etc.

System vulnerabilities

Source 1 : The Daily Swig (https://www.bleepingcomputer.com/)
https://portswigger.net/daily-swig/critical-rce-account-takeover-flaws-patched-in-rock-rms-church-management-platform?&web_view=true
Impact value: Critical

Rock RMS account takeover flaw. Rock RMS, a relationship management system for churches has patched a pair of critical vulnerabilities that can lead to account takeover and remote code execution issues. These flaws are tracked as CVE-2019-18642 and CVE-2019-18643 and score a rating of 9.8 on the CVSS scale.

Source 2 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/hackers-start-exploiting-recently-disclosed-zyxel-vulnerability
Impact value: Critical

Hackers Exploiting Recently Disclosed Zyxel Vulnerability. Security researchers have observed the first attempts of exploiting Zyxel devices using a recently disclosed vulnerability, CVE-2020-29583. The flaw, that affects several Zyxel firewalls and WLAN controllers, arises due to the hardcoded credentials stored in the firmware.

Malware

Source 1 : The Hacker News (https://thehackernews.com/)
https://thehackernews.com/2021/01/warning-cross-platform-electrorat.html
Impact value: High

Cross-Platform ElectroRAT Malware Targeting Cryptocurrency Users. Cybersecurity researchers today revealed a wide-ranging scam targeting cryptocurrency users that began as early as January last year to distribute trojanized applications to install a previously undetected remote access tool on target systems. Called ElectroRAT by Intezer, the RAT is written from ground-up in Golang and designed to target multiple operating systems such as Windows, Linux, and macOS. The apps are developed using the open-source Electron cross-platform desktop app framework.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/
Impact value: High

Babuk Locker is the first new enterprise ransomware of 2021. Babuk Locker is a new ransomware operation that launched at the beginning of 2021 and has since amassed a small list of victims from around the world. From ransom negotiations with victims seen by BleepingComputer, demands range from $60,000 to $85,000 in Bitcoin. Each Babuk Locker executables analyzed by BleepingComputer has been customized on a per-victim basis to contain a hardcoded extension, ransom note, and a Tor victim URL.

Botnets/DDoS

Source : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/citrix-adds-netscaler-adc-setting-to-block-recent-ddos-attacks/

Impact value: Informative

Citrix adds NetScaler ADC setting to block recent DDoS attacks. Citrix has released a feature enhancement designed to block attackers from using the Datagram Transport Layer Security (DTLS) feature of Citrix ADC and Gateway devices as an amplification vector in DDoS attacks. DTLS is a UDP-based version of the Transport Layer Security (TLS) protocol utilized to secure and to prevent eavesdropping and tampering in delay-sensitive apps and services. According to reports that have surfaced starting with December 21st, 2020, a DDOS attack used DTLS to amplify traffic from susceptible Citrix ADC devices dozens of times.

Spam & Phishing

Source : 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 1 : Threat Post (https://threatpost.com//)
https://threatpost.com/researcher-breaks-recaptcha-speech-to-text-api/162734/
Impact value: Informative
reCAPTCHA v3 cracked. Researchers have released a PoC for a previously discovered reCAPTCHA v3 attack method that uses voice-to-text to bypass CAPTCHA protection. The attack method, which has a success rate of 97 percent, works by collecting the MP3 file of the audio reCAPTCHA and submitting it to Google's own speech-to-text API. The attack method can be leveraged by attackers to collect sensitive data from browsers.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com//)
https://www.bleepingcomputer.com/news/security/indian-government-sites-leaking-patient-covid-19-test-results/
Impact value: High
Indian government sites leaking patient COVID-19 test results. Websites of multiple Indian government departments, including national health and welfare agencies, are leaking COVID-19 lab test results for thousands of patients online. These leaked lab reports which are being indexed by search engines expose patient data, and whether they tested positive for coronavirus.

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 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/google-releases-january-2021-security-updates-android
9**Impact value: Informative**
Google addresses 42 flaws. Google has announced fixes for 42 vulnerabilities affecting its Android devices, as part of January 2021 security updates. Four of these flaws are rated critical and affect Android's system component and Media Framework.

www.ke-cirt.go.ke