NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
4TH 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	2	0	1
System Vulnerabilities	0	1	0	0
Malware	0	2	0	0
DDoS/Botnets	0	0	0	1
Spam & Phishing	0	1	0	0
Web Security	0	1	0	0
Updates & Alerts	0	1	0	1

Top Stories

Source 1 : ZDnet (https://www.zdnet.com/)
https://www.zdnet.com/article/solarwinds-hackers-accessed-microsoft-source-code/
Impact value: High

Over 200 million records on sale. Over 200 million records related to Chinese citizens have been put on sale on a Russian dark web forum. The exposed data includes ID, gender, name, birth date, mobile number, address, and code numbers of citizens. Researchers claim that the data might have been stolen from multiple popular Chinese services, including Gongan, County, Weibo, and QQ.

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/microsoft/microsofts-unreleased-windows-core-polaris-os-leaks-online/
Impact value: Informative

Windows Core Polaris code leaked. Microsoft’s unreleased Windows Core Polaris OS was reportedly been leaked online. However, the good news is that the leak included a very early build from 2018 and contained no shell or apps.

https://www.bleepingcomputer.com/news/security/translink-confirms-ransomware-data-theft-still-restoring-systems/
Impact value: Informative

TransLink confirms ransomware data theft, still restoring systems. Metro Vancouver's transportation agency TransLink has confirmed that the Egregor ransomware operators who breached its network at the beginning of December 2020 also accessed and potentially stole employees' banking and social security information.

System vulnerabilities

Source : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/zend-framework-remote-code-execution-vulnerability-revealed/

Impact value: High

Zend Framework remote code execution vulnerability revealed. An untrusted deserialization vulnerability disclosed this week in how Zend Framework can be exploited by attackers to achieve remote code execution on PHP sites. This vulnerability tracked as CVE-2021-3007 may also impact some instances of Laminas Project, Zend's successor. Zend Framework consists of PHP packages installed over 570 million times. The framework is used by developers to build object-oriented web applications. This week, security researcher Ling Yizhou has disclosed how a particular gadget chain in Zend Framework 3.0.0 can be abused in untrusted deserialization attacks. If exploited, the flaw can allow remote attackers to conduct remote code execution (RCE) attacks on vulnerable PHP applications under certain circumstances.

Malware

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/

Impact value: High

APT27 turn to ransomware. In an extended investigation, security researchers have found that the China-based APT27 threat actor group is behind ransomware attacks that targeted at least five companies in the online gambling sector. For this, the attackers relied on the BitLocker encryption tool and Clambling backdoor, a malware sample similar to the one used in the DBRControl campaign. Other malware found in the attack campaign includes the PlugX RAT.

Source 2 : Security Affairs (https://securityaffairs.c/)
https://securityaffairs.co/wordpress/112972/hacking/muddywater-attack-github-imgur.html?web_view=true

Impact value: High

New alleged MuddyWater attack downloads a PowerShell script from GitHub. Security expert discovered a new piece of malware uses weaponized Word documents to download a PowerShell script from GitHub. This PowerShell script is also used by threat actors to download a legitimate image file from image hosting service Imgur and decode an embedded Cobalt Strike script to target Windows systems. The researcher Arkbird published technical details of the malware that uses steganography to hide the malicious code in the image. Arkbird pointed out that the sample could be part of the Muddywater APT's arsenal.

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 : Info Security (https://www.infosecurity-magazine.com//)
https://www.infosecurity-magazine.com/news/one-million-compromised-accounts/?&web_view=true

Impact value: High

One Million Compromised Accounts Found at Top Gaming Firms. Security researchers have warned gaming companies to improve their cybersecurity posture after discovering 500,000 breached employee credentials and a million compromised internal accounts on the dark web. Tel Aviv-based threat intelligence firm Kela decided to investigate the top 25 publicly listed companies in the sector based on revenue. After scouring dark web marketplaces, it discovered a thriving market in network access on both the supply and demand side. This included nearly one million compromised accounts related to employee- and customer-facing resources, half of which were listed for sale last year. Compromised accounts linked to internal resources like admin panels, VPNs, Jira instances, FTPs, SSOs, developer-related environments and more were found in virtually all of the top 25 gaming companies studied. This could put these firms at risk of customer data theft, corporate espionage, ransomware and more. Kela said it had tracked ransomware attacks on four gaming companies in recent months.

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 : Ciso Mag (https://cisomag.eccouncil.org/)
https://cisomag.eccouncil.org/microsoft-source-code-viewed-in-solarwinds-hack/
Impact value: Informative

New update on SolarWinds. Microsoft has issued an update in which it has confirmed that it traced a compromised account used to “view source code” of its internal code structure. However, it stated that viewing source code is not tied to an elevation of risk.

www.ke-cirt.go.ke