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

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

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

https://www.zdnet.com/article/joomla-team-discloses-data-breach/

Impact value: Informative

Maintainers at the Joomla open-source content management system (CMS) announced a security breach that took place last week. Last week a member of the Joomla Resources Directory (JRD) team left an unencrypted full backup of the JRD site (resources.joomla.org) on an unsecured Amazon Web Services S3 bucket operated by the company. The backup contained details for approximatively 2,700 users who registered and created profiles on the JRD website.

https://www.zdnet.com/article/amtrak-discloses-data-breach-potential-leak-of-sensitive-customer-information/

Impact value: Informative

Even with the travel restrictions prompted by the COVID-19 pandemic, the travel industry is once again tainted by a security incident that resulted in the leak of personal identifiable information found in Amtrak's Guest Rewards service. According to a Notice of Data Breach sent to the Attorney General's Office of Vermont, The National Railroad Passenger Corporation discovered the security incident on April 20. "On the evening of April 16, 2020, Amtrak determined that an unknown third party gained unauthorized access to certain Amtrak Guest Rewards accounts," the letter reads. Although the company didn't say how many account were breached, the notification states that "compromised usernames and passwords were used to access certain accounts and some personal information may have been viewed."

System vulnerabilities

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/vmware-cloud-director-flaw-lets-hackers-take-over-virtual-datacenters/

Impact value: Critical

Cybersecurity researchers today disclosed details for a new vulnerability in VMware's Cloud Director platform that could potentially allow an attacker to gain access to sensitive information and control private clouds within an entire infrastructure. Tracked as CVE-2020-3956, the code injection flaw stems from an improper input handling that could be abused by an authenticated attacker to send malicious traffic to Cloud Director, leading to the execution of arbitrary code. It's rated 8.8 out of 10 on the CVSS v.3 vulnerability severity scale, making it a critical vulnerability. VMware Cloud Director is a popular deployment, automation, and management software that's used to operate and manage cloud resources, allowing businesses to data centers distributed across different geographical locations into virtual data centers.

Malware

Source 1 : Security Affairs (https://securityaffairs.co/)
https://securityaffairs.co/wordpress/104149/cyber-crime/sodinokibi-published-elexon-files.html
Impact value: Medium
Elexon, a go-between in the UK power grid network, was the victim of a cyber attack in May. Its systems had been infected with the Sodinokibi ransomware. Elexon company is an electricity-regulating company regulating electricity quota and applying it around the network according to demand. This hack affected the company's internal IT network, along with employees' laptops and email servers. However, they spared the system responsible for the UK electricity transit, BSC Central Systems, and EMR. After taking down email servers in response to the attack, the company released a message declaring that they located the root source of the incident and was working to restore the internal network and employee laptops. Two weeks after the declaration, Sodinokibi released the leaked data; a total of 1,280 files, including the passports of Elexon staff members and an evident business insurance application form, on their leak site.

Spam & Phishing

Source 1 : Tech Republic (https://www.techrepublic.com/)
https://www.techrepublic.com/article/covid-19-emergence-leads-to-37-jump-in-mobile-phishing-attacks-in-2020/

Impact value: Informative

Lookout, Inc., a leader in mobile security, released its 2020 Mobile Phishing Spotlight Report that reveals there was a 37 percent increase worldwide in enterprise mobile phishing encounter rate between the fourth quarter of 2019 and the first quarter of 2020. The report also shows that unmitigated mobile phishing threats could cost organizations with 10,000 mobile devices as much as $35 million per incident, and up to $150 million for organizations with 50,000 mobile devices.

Web Security

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

https://www.bleepingcomputer.com/news/software/firefox-77-rolls-out-webrender-to-more-windows-10-laptops/

Impact value: Informative

Firefox 77, the latest stable version of the browser from Mozilla, started rolling out today. It brings a whole bunch of functional features and fixes. Notably, the latest version pushes WebRender to more users of Firefox for Windows 10. Mozilla is developing the feature to improve browser stability and performance. With WebRender, Firefox should offer superior frame rates. In turn, the feature lets applications run smoothly on the browser. The tech is a work in progress, however, and to date, it's still not available to all Firefox users.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)

https://www.us-cert.gov/ncas/bulletins/sb20-153

Vulnerability Summary for the Week of May 25, 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: Security Affairs (https://securityaffairs.co)

https://securityaffairs.co/wordpress/104168/hacking/apple-fixes-cve-2020-9859-jailbreak.html

Impact value: High

The zero-day vulnerability tracked as CVE-2020-9859 is exploited by the "Uncover" jailbreak tool released last week. Apple quietly pushed out a small but important update for operating systems across all of its devices, including a patch for a zero-day exploit used in an iPhone jailbreak tool released last week. In its notes for the release, Apple says very little else about the patches overall that it pushed out Monday — for iOS (including 13.4.6 for HomePod) and iPadOS 13.5.1, watchOS 6.2.6, tvOS 13.4.6, and macOS 10.15.5 — other than that they provide "important security updates" that are "recommended for all users."

Source 2: cisco (https://tools.cisco.com)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ipip-dos-kCT9X4

Impact value: High

Cisco has patched a high-severity flaw in its NX-OS software, the network operating system used by Cisco's Nexus-series Ethernet switches. If exploited, the vulnerability could allow an unauthenticated, remote attacker to bypass the input access control lists (ACLs) configured on affected Nexus switches – and launch a denial of service (DoS) attacks on the devices.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke