NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
3rd September 2019

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

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

https://cyware.com/news/xkcd-forum-hit-with-data-breach-exposing-information-of-over-500000-members-7ef17f88

XKCD forum hit with data breach exposing information of over 500,000 members. XKCD forum has been taken offline following a security breach that occurred two months ago. The incident has affected the personal information of more than 562,000 members. The exposed information includes usernames, email addresses, hashed passwords, and in some cases an IP address of users.

https://cyware.com/news/unprotected-database-of-flight-booking-site-option-way-exposes-sensitive-customer-information-6ca9b95c

Unprotected database of flight booking site Option Way exposes sensitive customer information. A leaky database associated with Option Way, a France-based flight booking website, was found leaking over 100GB of data. This included customers' names, birth dates, gender, email addresses, phone numbers, home addresses, destinations, flight prices, and other sensitive details.

https://cyware.com/news/foxit-software-suffers-data-breach-impacting-over-328k-accounts-d0136162

Foxit Software suffers data breach impacting over 328K accounts. PDF software provider Foxit Software suffered a data breach after unauthorized third parties gained access to its data systems including 'My Account' user data. The compromised 'My Account' user data includes usernames, email addresses, company names, phone numbers, user account passwords, and user IP addresses.

System vulnerabilities

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

https://www.zdnet.com/article/over-47000-supermicro-servers-are-exposing-bmc-ports-on-the-internet/

Over 47,000 Supermicro servers are exposing BMC ports on the internet. A new set of vulnerabilities named USBAnywhere has been found impacting the baseboard management controller (BMC) firmware of Supermicro motherboards. This has opened more than 47,000 workstations and servers running on Supermicro motherboards to cyberattacks. Patches are available to fix the vulnerabilities which include plaintext authentication, unencrypted network traffic, weak encryption, and authentication bypass.

Source 2: Tenable (https://www.tenable.com/)

https://www.tenable.com/plugins/nessus/128063

Cisco Adaptive Security Appliance VPN SAML Authentication Bypass Vulnerability (cisco-sa-20190501-asaftd-saml-vpn). Cisco has released security patches to fix vulnerabilities impacting its Adaptive Security Appliance (ASA) and NX-OS software. Both the software are affected by authentication bypass vulnerability (CVE-2019-1714) and arbitrary file overwrite vulnerability (CVE-2019-1729) respectively.

Malware

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

https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-via-fake-forums-on-hacked-sites/

Sodinokibi Ransomware Spreads via Fake Forums on Hacked Sites. A hacker has been found hacking WordPress sites with an intent to distribute Sodinokibi ransomware. The hacked websites are injected with malicious JavaScripts that overlay the actual content and display a fake Q&A forum post to visitors. These fake 'answer' posts contain a link to the ransomware installer.

https://www.bleepingcomputer.com/news/security/nemty-ransomware-gets-distribution-from-rig-exploit-kit/

Nemty Ransomware Gets Distribution from RIG Exploit Kit. The newly discovered Nemty ransomware, which appeared on the radar towards the end of August, is now distributed in malvertising campaigns using the RIG exploit kit. The malware uses the .nemty extension to append the encrypted files. Later, it displays a ransom note which provides instructions on how to pay to recover the data.

https://www.bleepingcomputer.com/news/security/astaroth-trojan-uses-cloudflare-workers-to-bypass-av-software/

Astaroth Trojan Uses Cloudflare Workers to Bypass AV Software. Security researchers have uncovered a new variant of Astaroth trojan that is distributed by abusing the Cloudflare Workers' serverless computing platform. This enables the attackers to avoid detection while spreading its infection process. The variant is delivered in JSON format depending on the target's location.

Malware

https://www.bleepingcomputer.com/news/security/fake-bleachbit-website-built-to-distribute-azorult-info-stealer/

Fake BleachBit Website Built to Distribute AZORult Info Stealer. Cybercriminals have created a fake BleachBit website in order to spread the AZORult information stealing trojan. Once installed, the trojan contacts the C2 server for instructions and collects browser history, login credentials, cookies and files in specific locations.

DDoS/Botnets

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

https://www.zdnet.com/article/new-cryptojacking-campaign-strikes-half-a-million-pcs/

Smominru hijacks half a million PCs to mine cryptocurrency, steals access data for Dark Web sale. Smominru botnet has been updated to go far beyond cryptomining. It is now capable of stealing information from vulnerable targets. The botnet was used in a cyberespionage campaign that infiltrated nearly 500,000 systems worldwide. Smominru has been active since 2017 and is generally distributed using EternalBlue exploit kit.

Spam & Phishing

Source 1: FossBytes (https://fossbytes.com/)

https://fossbytes.com/scammers-use-ai-to-fake-ceos-voice-transfer-243000/

Scammers Use AI To Fake CEO's Voice, Transfer $243,000. Fraudsters have found a new form of vishing attack that enabled them to drain out around $243,000 from an energy firm. They leveraged an AI-based software to fake the voice of the CEO of a UK-Based energy firm and tricked the targeted employees. The fraudsters had asked the employees to transfer the money to a Hungary-based supplier in an hour and promised to refund it soon. However, the money was never refunded and another money transfer demand was placed using the same tactic.

Web security

Source 1: infoSecurity (https://www.infosecurity-magazine.com/)

https://www.infosecurity-magazine.com/news/data-leak-affects-25m-customers/

Data Leak Hits 2.5 Million Customers of Cosmetics Giant Yves Rocher. An unprotected Elasticsearch database belonging to Aliznet has exposed the personal data of over 2.5 million Yves Rocher customers. The compromised data includes first and last names, phone numbers, email addresses, birth dates and zipcode of customers. In addition to this, the database has also exposed internal data related to the cosmetic firm which includes store traffic, turnover, and order volumes.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb19-245
Vulnerability Summary for the Week of August 26, 2019. 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/technetwork/security-advisory/cpujul2019-5072835.html
Oracle Critical Patch Update Pre-Release Announcement - July 2019; advised action to run available security updates.

https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.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/technetwork/topics/security/bulletinjul2019-5600410.html
Oracle Solaris Third Party Bulletin - July 2019; advised action to apply necessary patches.

https://www.oracle.com/technetwork/topics/security/linuxbulletinjul2019-5600392.html
Oracle Linux Bulletin - July 2019; advised action to apply necessary Oracle Linux Bulletin fixes.

https://www.oracle.com/technetwork/topics/security/public-vuln-to-advisory-mapping-093627.html
Map of CVE to Advisory/Alert; advised action to apply the critical patch update for protection against known vulnerabilities.

https://www.oracle.com/technetwork/topics/security/ovmbulletinjul2019-5600406.html
Oracle VM Server for x86 Bulletin - July 2019; advised action to apply necessary Oracle VM Server for x86 Bulletin fixes.

Updates & Alerts

Source 1: Cisco Security Advisories & Alerts(http://tools.cisco.com/security/center/publicationListing.x)

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

Cisco Secure Boot Hardware Tampering Vulnerability. Due to an improper check on the area of code that manages on-premise updates to a Field Programmable Gate Array (FPGA) part of the Secure Boot hardware implementation an authenticated, local attacker could write a modified firmware image to the component.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke