NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
10th September 2019

COMMUNICATIONS
AUTHORITY OF KENYA

Summary Headlines	Impact Metric Against Count of Events			
	Critical	High	Medium	Informative
Top Stories	1	0	0	2
System vulnerabilities	1	1	0	0
Malware	2	1	0	0
DDoS/Botnets	1	0	0	0
Spam & phishing	0	1	0	0
Web Security	1	1	0	0
Updates & alerts	0	1	0	2

Top Stories

Source 1: ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/
Impact value: Informative

Security researchers expose another instance of Chrome patch gapping. Patch gapping is a relatively new technical term used to describe gaps in the patching process of software that relies on open-source components. Security researchers have found another instance of patch gapping in the Google Chrome browser that could have been abused by hackers to develop exploits and launch attacks against Chrome users days before a patch would have been readily available for everyone.

https://www.zdnet.com/article/cyber-security-incident-at-us-power-grid-entity-linked-to-unpatched-firewalls/
Impact value: Critical

Cyber-security incident at US power grid entity linked to unpatched firewalls. New details about cybersecurity incidents impacting a US power grid entity earlier this year have emerged recently. In a report, the North American Electric Reliability Corporation (NERC) has highlighted that the incident occurred due to a DoS flaw in firewalls. This caused the attackers to reboot the firewall for about ten hours.

Top Stories

Source 2: The Register (https://www.theregister.co.uk/)
https://www.theregister.co.uk/2019/09/09/mozilla_firefox_dns/
Impact value: Informative

Mozilla Firefox to begin slow rollout of DNS-over-HTTPS by default at the end of the month. DNS-Over-HTTPS (DoH) transfers domain name system queries, that try to match domain names with server IP addresses, over an encrypted HTTPS connection rather than an unprotected HTTP one. Firefox's DoH service will be provided through Cloudflare's 1.1.1.1 DNS service.

System vulnerabilities

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

https://cyware.com/news/new-exim-vulnerability-opens-up-millions-of-email-servers-to-root-granting-exploitation-911f3f1a
Impact value: Critical

New Exim vulnerability opens up millions of email servers to root-granting exploitation. All Exim servers running versions prior to 4.92.1 are vulnerable to a security flaw that can grant attackers the ability to run malicious code with root privileges. The vulnerability has been tracked as CVE-2019-15846 and can be mitigated with the latest 4.92.2 version.

Source 2: Threat Post (https://threatpost.com/)
https://threatpost.com/psixbot-pornmodule-google-dns/148142/
Impact value: High

PsiXBot Adds PornModule, Google DNS Service to Its Arsenal. PsiXBot is a multi-use Windows malware that has a range of capabilities, including keylogging, stealing passwords and cookies, spreading spam, mining for cryptocurrency and fingerprinting infected machines. It has added new tricks including implementing Google's DNS over HTTPS (DoH) and adding the blackmail-ready "PornModule".

Malware

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

https://cyware.com/news/uscyber-command-releases-11-malware-samples-linked-with-north-korean-government-hackers-2f1e38e1/
Impact value: Critical

U.S. Cyber Command releases 11 malware samples linked with North Korean government hackers. U.S. Cyber Command has shared 11 malware samples on VirusTotal, which are believed to be linked with North Korean threat actor groups. Most of the samples share similarities with HOPLIGHT malware and are tied with the Lazarus threat actor group. HOPLIGHT is a Trojan that is primarily involved in gathering information from victims' systems.

https://cyware.com/news/linux-servers-under-attack-by-lilocked-ransomware-e9c4f966
Impact value: High

Linux servers under attack by Lilocked ransomware. A new ransomware strain tracked as Lilocked has been found actively targeting vulnerable Linux servers and encrypting the data stored on them. The malware leverages an Exim exploit to target servers. Once installed, it appends the encrypted files with .lilocked extension and later drops a ransom note named #README.lilocked.

Source 2: Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/exploit-kits-target-windows-users-with-ransomware-and-trojans/
Impact value: Critical

Exploit Kits Target Windows Users with Ransomware and Trojans. Four different malvertising campaigns have been redirecting users to exploit kits landing pages that install password stealing Trojans through Ramnit banking trojan, ransomware as the Nemty Ransomware and clipboard hijackers.

DDoS/Botnets

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

https://cyware.com/news/wikipedia-goes-partly-offline-after-massive-ddos-attack-4f7de6c9

Impact value: Critical

Wikipedia goes partly offline after massive DDoS attack. Wikipedia has suffered a massive DDoS attack, impacting its website across various countries. The attack occurred between September 6 and September 7, 2019. The impacted countries include the UK, France, Germany, Italy, the Netherlands, Poland, and parts of the Middle East.

Spam & Phishing

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

https://www.bleepingcomputer.com/news/security/microsoft-phishing-page-uses-captcha-to-bypass-automated-detection/

Impact value: High

Microsoft Phishing Page Uses Captcha to Bypass Automated Detection. Captchas are challenge-based methods to determine if the user is human or a bot. Their purpose is to prevent abuse and are typically found on registration pages to prevent automated sign up action. A new phishing campaign is using this type of challenge to block automated URL analysis from processing the dangerous page hiding a fake Microsoft account login page from Secure Email Gateways (SEGs).

Web security

Source 1: The Hacker News (https://thehackernews.com/)

https://thehackernews.com/2019/09/stealthfalcon-virus-windows-bits.html

Impact value: High

New Malware Uses Windows BITS Service to Stealthy Exfiltrate Data. Researchers have uncovered that PowerShell-based backdoor used by the Project Raven threat actor group is similar to the Win32/StealthFalcon backdoor of the Stealth Falcon group. The PowerShell-based backdoor is delivered via a weaponized document included in a malicious email.

Source 2: ZDNet (https://www.zdnet.com/)

https://www.zdnet.com/article/critical-vulnerabilities-impact-over-a-million-iot-radio-devices/

Impact value: Critical

Telnet backdoor vulnerabilities impact over a million IoT radio devices. Two critical vulnerabilities have been found impacting Telestar Digital GmbH IoT radio devices. The vulnerabilities have been assigned CVE IDs, CVE-2019-13473 and CVE-2019-13474. These flaws can allow attackers to remotely hijack systems.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://www.us-cert.gov/ncas/bulletins/sb19-252
Vulnerability Summary for the Week of September 2, 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

Impact value: High

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 attacker could write a modified firmware image to the component.

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

https://www.bleepingcomputer.com/news/microsoft/office-365-atp-automated-incident-response-now-generally-available/

Impact value: Informative

Office 365 ATP Automated Incident Response Now Generally Available. Microsoft announced the general availability of the Automated Incident Response feature in Office 365 Advanced Threat Protection (ATP) users to support the rising requirements of security teams by matching security teams' workflows to make it a lot faster to methodically address the most frequently encountered threats.

Updates & Alerts

Source 3: SC Magazine (https://www.scmagazine.com/)
https://www.scmagazine.com/website-web-server-security/wordpress-update-fixes-assortment-of-xss-flaws/
Impact value: Informative

WordPress update fixes assortment of XSS flaws. The developers of WordPress last week issued a short-cycle maintenance release for its content management system software, introducing 29 fixes and improvements.

www.ke-cirt.go.ke