NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
8th February 2021

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	1	0	0
Malware	0	0	1	0
DDoS/Botnets	0	0	1	0
Spam & Phishing	0	0	1	0
Web Security	0	0	0	2
Updates & Alerts	0	1	0	0

Top Stories

Source 1 : ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/government-censorship-threats-over-tiktok-spiked-interest-in-vpns/
Impact value: Informative
Consumer interest in VPN services saw a huge spike last year as users grew increasingly concerned about apps like TikTok being banned as well as securing their data while working from home during lockdown. While people use VPNs in order to bypass government restrictions, secure their home networks and hide their online activities from ISPs, new research from Security.org has revealed major news events from 2020 had a direct correlation with interest in VPN services.

Source 2 : ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/domestic-kitten-hacking-group-strikes-local-citizens-considered-a-threat-to-iranian-regime/
Impact value: Informative
Iran is running two surveillance operations in cyber-space, targeting more than 1,000 dissidents, according to a leading cyber-security company. The efforts were directed against individuals in Iran and 12 other countries, including the UK and US, Check Point said. It said the two groups involved were using new techniques to install spyware on targets' PCs and mobile devices.

System vulnerabilities

Source 1 : ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/with-one-update-this-malicious-android-app-hijacked-10-million-devices/
Impact value: High
Google Play has been battling malicious apps for years, and the most recent to sneak into the Play Store has hijacked roughly 10 million devices. The application in question is a popular barcode scanner app that was transformed into malware with one update. The app had been available on the app repository for several years, racking up 10 million installs. The application functions as a QR code reader and barcode generator that appeared to be legitimate and trustworthy software.

Source 2 : Threat Post (https://threatpost.com/)
https://threatpost.com/google-chrome-zero-day-windows-mac/163688/
Impact value: Critical
Google has released a warning to its customers stating that a zero-day vulnerability is being actively exploited by attackers and encouraging Google Chrome browser users to maintain aware of the issue and implement a patch as soon as it is available. The flaw lies in the V8 open-source web engine and affects version 88 of the popular browser on Mac, Windows, and Linux devices. Google stated that the flaw stems from a heap-buffer overflow, a type of buffer overflow error in which the region of a process’ memory can suffer from an overflow of data.

Malware

Source 1 : Security Week (https://www.securityweek.com/)
https://www.securityweek.com/packaging-giant-westrock-says-ransomware-attack-hit-production
Impact value: Medium

WestRock, an Atlanta based packaging giant announced on Friday that they had been the victims of a recent ransomware attack that impacted the company’s ability to operate, its information technology (IT), and operational technology (OT) systems. The company has simultaneously been investigating the incident while attempting to restore affected systems. WestRock has responded to the attack proactively by shutting down certain systems and enhancing cybersecurity measures on others that remain in operation. Although the incident impacted production efforts, WestRock is now almost back to normal in terms of business operations. Staff are performing some automated tasks manually until systems are restored.

Botnets/DDoS

Source 1 : The Daily Swig (https://portswigger.net/)
https://portswigger.net/daily-swig/ransom-related-ddos-attacks-rise-from-the-dead-as-attack-vectors-diversify
Impact value: Medium
New evidence suggests that there has been a significant increase in the number of ransom-related DDoS (RDDoS) attacks during the COVID-19 crisis. A report by US tech firm Neustar found that RDDoS attacks rose by 154% across 2020. RDDoS attacks involve a threat actor attempting to extort money from an individual or organization by threatening them with disruption caused by a DDoS attack.

Spam
&
Phishing

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/
Impact value: Medium
A new phishing attack has been discovered making use of a form of communication that is more commonly associated with 19th-century radio signals than modern cyberattacks: Morse code. The campaign uses Morse code to enable malicious login forms to escape detection by anti-phishing email software.

Web Security

Source 1 : Google Cloud (https://cloud.google.com/)
https://cloud.google.com/blog/topics/developers-practitioners/search-and-browse-google-cloud-code-samples

Impact value: Informative

Google Cloud has added a number of new features that should make it easier for cloud computing developers to start new projects. In particular, it should be more straightforward for them to find existing code samples, which they can then use or tweak for their own software solutions.

Source 2 : 9to5mac (https://9to5mac.com/)
https://9to5mac.com/2021/02/05/microsoft-officially-launches-autofill-password-manager-for-ios-and-other-platforms/amp/

Impact value: Informative

Microsoft has officially launched its password manager Autofill solution, making it available through the Microsoft Authenticator app. Although the tool was already available as part of Microsoft's beta program, it will now be accessible to anyone with a Microsoft account, whether they use Windows PCs, Macs, Android, or iOS devices.

Bulletins

Source 1: US-CERT - Security Bulletin Mailing List (http://www.us-cert.gov/cas/bulletins/)
https://us-cert.cisa.gov/ncas/bulletins/sb21-032
Vulnerability Summary for the Week of January 25, 2021. 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/cpujul2020.html
Oracle Critical Patch Update Advisory - July 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, a deserialization vulnerability via XMLDecoder in Oracle WebLogic Server Web Services; advised action to run security updates.

https://www.oracle.com/security-alerts/bulletinjul2020.html
Oracle Solaris Third Party Bulletin - July 2020; advised action to apply necessary patches.

https://www.oracle.com/security-alerts/linuxbulletinjul2020.html
Oracle Linux Bulletin - July 2020; 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/ovmbulletinjul2020.html
Oracle VM Server for x86 Bulletin - July 2020; advised action to apply necessary Oracle VM Server for x86 Bulletin fixes.

Updates & Alerts

Source 1 : Beta News (https://betanews.com/)

https://betanews.com/2021/02/07/windows-10-updates-kb4598299-kb4598301-visual-studio-problems/

Impact value: High

It looks like Microsoft is still struggling with releasing Windows 10 updates that appear to break more than they fix. Recently, the company released the cumulative KB4598291 update, which was meant to fix several bugs that have been hanging around since the October 2020 Update. While it appears that most of these issues are now fixed, it seems like the update has a few problems of its own.

www.ke-cirt.go.ke