NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
9th 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	2	0	0	0
Malware	0	1	1	0
DDoS/Botnets	0	0	0	0
Spam & Phishing	0	0	1	0
Web Security	0	0	0	1
Updates & Alerts	0	1	0	0

Top Stories

Source 1 : Info Security (https://www.infosecurity-magazine.com/)
https://www.infosecurity-magazine.com/news/europol-breaks-14-million-card/
Impact value: Informative

Europol claims to have dismantled an organized crime group that had swindled US banks out of $14.4 million. According to Europol, the organization launched a single-day operation in which Spanish National Police and the US Secret Service conducted 40 house searches, arrested 37 suspects, and seized 13 cars. The day is nicknamed Operation Secreto and also consisted of freezing roughly 87 bank accounts. The scheme was traced back to Greek nationals, according to authorities.

Source 2 : Washington Post (https://www.washingtonpost.com/)
https://www.washingtonpost.com/nation/2021/02/08/researchers-find-more-victims-one-irans-oldest-hacking-groups/
Impact value: Informative

Two cyber threat groups have been identified and determined to be working for the Iranian government. One of the groups is called Infy and has been operating since at least 2007. Infy has been accused of perpetrating attacks against Persian language media, diplomatic targets, and Iranian dissidents in multiple countries such as the US and Canada. According to researchers at Check Point Security, an investigation determined that the Iranian government is still spying on the mobile phones and devices of dissidents and other individuals of interest to the regime.

System vulnerabilities

Source 1 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/critical-vulnerability-fixed-in-wordpress-plugin-with-800k-installs/
Impact value: Critical
The developers behind the NextGen Gallery plugin have fixed two critical Cross-site request forgery (CSRF) vulnerabilities, their exploitation could lead to a site takeover, malicious redirects, spam injection, phishing, and other malicious activities. The NextGEN Gallery is one of the most popular WordPress gallery plugins that is available since 2007. The plugin receives over 1.5 million new downloads per year, it easily allows to create highly responsive photo galleries

Source 2 : Bleeping Computer (https://www.bleepingcomputer.com/)
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-reader-vulnerability-exploited-in-the-wild/
Impact value: Critical
Adobe is warning of a critical vulnerability that has been exploited in the wild to target Adobe Reader users on Windows. The vulnerability (CVE-2021-21017) has been exploited in “limited attacks,” according to Adobe’s Tuesday advisory, part of its regularly scheduled February updates. The flaw in question is a critical-severity heap-based buffer overflow flaw. This type of buffer-overflow error occurs when the region of a process’ memory used to store dynamic variables (the heap) can be overwhelmed. If a buffer-overflow occurs, it typically causes the affected program to behave incorrectly. With this flaw in particular, it can be exploited to execute arbitrary code on affected systems.

Malware

Source 1 : Cyber Scoop (https://www.cyberscoop.com/)
https://www.cyberscoop.com/android-spying-bangladesh-talos/
Impact value: Medium

A newly discovered variant of the LodaRAT malware, which has historically targeted Windows devices, is being distributed in an ongoing campaign that now also hunts down Android devices and spies on victims. Along with this, an updated version of LodaRAT for Windows has also been identified; both versions were seen in a recent campaign targeting Bangladesh, researchers said.

Source 2 : ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/cd-projekt-red-game-studio-discloses-ransomware-attack-extortion-attempt/
Impact value: High

CD Projekt Red has been hacked, with several company documents and source codes for their games being stolen and held under ransom. The Cyberpunk 2077 developers announced that the hacking had taken place on Twitter, also sharing the rather cringy ransom note left behind by the hackers. The note claims that the source code for Cyberpunk 2077, Witcher 3, Gwent, and an unreleased version of Witcher 3 has been stolen. Documents relating to accounting, administration, legal, HR, investor relations, "and more" are also allegedly compromised.

Spam
&
Phishing

Source 1 : The Verge (https://www.theverge.com/)
https://www.theverge.com/2021/2/8/22272849/apple-app-store-scams-ios-fraud-reviews-ratings-flicktype?scrolla=5eb6d68b7fedc32c19ef33b4
Impact value: Medium

Apple's App Store may be playing host to a number of scam apps that are raking in millions for criminals across the world, a developer has claimed. Kosta Eleftheriou says that a host of malicious apps are present on the App Store, and has accused Apple of failing to act and protect its users. Many of the scam apps follow the same formula, Eleftheriou says, with fake reviews and ratings helping to boost their status on the App Store and lure in more vicitims.

Web Security

Source 1 : Windows Latest (https://www.windowslatest.com/)
https://www.windowslatest.com/2021/02/09/windows-10-may-soon-tell-you-which-apps-are-using-your-camera/
Impact value: Informative
Windows 10 could soon get a new feature that will make using your webcam more secure, with Microsoft testing a setting that lets you known when your camera is in use – and which apps are using it. When your webcam is in use, an icon will appear in the taskbar alerting you. If you hover over the icon, a list will appear showing you all the apps that are currently using your webcam.

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 : 9to5mac (https://9to5mac.com/)
https://9to5mac.com/2021/02/08/psa-upgrading-a-mac-to-macos-big-sur-without-enough-space-can-result-in-data-loss/
Impact value: High

Mac owners who are upgrading to macOS Big Sur should be very careful if they are running low on drive space, as in this case, the process could reportedly lead to data loss. The issue here is that an initial upgrade to Big Sur requires a minimum of 35.5GB to be available on the drive, plus 13GB for the macOS Big Sur installer itself (making 48.5GB in total). If you don’t have that much space, then things can go badly wrong, as reported by Mr Macintosh.

www.ke-cirt.go.ke