NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
22nd 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	0	1	0	0
Malware	0	0	0	2
DDoS/Botnets	0	0	0	0
Spam & Phishing	0	0	0	1
Web Security	0	0	0	1
Updates & Alerts	0	0	0	1

COMMUNICATIONS AUTHORITY OF KENYA

Top Stories

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

https://www.bleepingcomputer.com/news/security/hacker-arrested-for-stealing-selling-pii-of-65k-hospital-employees/

Impact value: Informative

Justin Sean Johnson, a 29-year-old man from Michigan, was arrested earlier this week for his involvement in a 2014 hack of the health care provider University of Pittsburg Medical Center (UPMC). Johnson allegedly executed the attack and stole personally identifiable information and W-2 information of over 65,000 employees. Johnson is accused of selling sensitive stolen data on the dark web after the attack. UPMC is Pennsylvania's largest healthcare provider, boasting over 90,000 employees, 40 hospitals, and 700 outpatient sites. Earlier this week, Johnson was charged in a forty-three count indictment that includes aggravated identity theft, wire fraud, and conspiracy. In a press release, US Attorney Brady stated that Johnson is accused of stealing the names, SSN, addresses, and salary information of every UPMC employee. Brady also stated that the information sold by Johnson on the dark web was later used to engage in massive phishing campaigns against these employees that resulted in further scams and theft.

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

https://www.zdnet.com/article/blueleaks-data-from-200-us-police-departments-fusion-centers-published-online/

Impact value: Informative

On Friday, an activist group that describes itself as a transparency collective published 296GB of data that appears to have been stolen from US law enforcement agencies and fusion centers. The massive data leak has been named BlueLeaks and was published by the group Distributed Denial of Secrets (DDoSecrets). The data claims to span more than 10 years of files belonging to over 200 police departments across the US.

System vulnerabilities

Source 1 : Threat Post (https://threatpost.com/)
https://threatpost.com/amd-fixes-for-high-severity-smm-callout-flaws-upcoming/156787/

Impact value: High

AMD recently announced that it was preparing patches for an SMM Callout Privilege Escalation vulnerability, tracked as CVE-2020-12890, that affects the System Management Mode (SMM) of the Unified Extensible Firmware Interface (UEFI). The vulnerability was discovered by the security researcher Danny Odler, it resides in the AMD's Mini PC could allow attackers to manipulate secure firmware and execute arbitrary code. The issue could be exploited by attackers only if they have privileged physical or administrative access to a system that includes one of the affected AMD notebook or embedded processors.

Malware

Source 1 : Techradar (https://www.techradarcom/)

https://www.techradar.com/au/news/hackers-have-turned-discord-into-an-account-stealer-heres-what-you-need-to-know

Impact value: Informative

Security researchers discovered a new malware threat called “NitroHack” that modifies the Discord client for Windows into an info stealing Trojan. MalwareHunterTeam observed malicious actors abusing DM’s from infected Discord users as a distribution vector. Specifically, they leveraged those accounts to inform a victim’s friends that they could obtain free access to the premium Discord Nitro service by downloading a file. By complying, a user inadvertently infected themselves with NitroHack. This malware appended malicious code to the “%AppData%\Discord.0.306modulesdiscord_voiceindex.js” file as well as attempted to change the same file in both the iscord Canary and Discord Public Test Build clients.

Source 2 : Security Affairs (https://securityaffairs.co/)

https://securityaffairs.co/wordpress/105049/malware/icedid-banking-trojan-steganography.html

Impact value: Informative

Juniper Threat Labs has been monitoring a campaign that pushes a new IcedID banking trojan. This new campaign changes tactics by injecting into msiexec.exe to conceal itself and use full steganography for downloading its modules and configurations. Previous versions of IcedID injected into svchost.exe and downloaded encrypted modules and config as “.dat” files. This campaign also takes advantage of the COVID-19 pandemic by using keywords such as COVID-19 and FMLA in email sender names and attachment names. IcedID is a banking malware that performs Man-in-the-Browser attacks to steal financial information.

Spam & Phishing

Source 1 : ZDNet (https://www.zdnet.com/)
https://www.zdnet.com/article/australians-reported-25000-phishing-scams-to-the-accc-last-year/

Impact value: Informative

Australians reported losing $2.5 billion to scammers over the past decade but actual losses were far larger because one-third of people who were ripped off did not report it, the competition watchdog says. In 2019, phishing was the most common method for scamming, with 25,168 reports. 513 of those reported resulted in a financial loss, valued at AU$1.5 million.

Web Security

Source 1 : Threat Post (https://threatpost.com/)

https://threatpost.com/adobe-prompts-users-to-uninstall-flash-player-as-eol-date-looms/156794/

Impact value: Informative

Adobe plans to prompt users and ask them to uninstall Flash Player from their computers by the end of the year when the software is scheduled to reach End-Of-Life (EOL), on December 31, 2020. The move was announced in a new Flash Player EOL support page that Adobe published earlier this month, six months before the EOL date. Adobe says that once Flash reached the EOL date, the company doesn't merely plan to stop providing updates, but they also plan to remove all Flash Player download links from their website.

Bulletins

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

https://www.us-cert.gov/ncas/bulletins/sb20-167

Vulnerability Summary for the Week of June 8, 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: Bleeping Computer (https://www.bleepingcomputer.com)

https://www.bleepingcomputer.com/news/microsoft/malwarebytes-causing-performance-issues-in-windows-10-2004/

Impact value: Informative

Following the release of Windows 10 2004, users have reported experiencing performance issues and even crashes when Malwarebytes 4.1 is installed on their systems. The official Malwarebytes support forum has seen numerous users reporting problems with MBAM 4.1 after Microsoft released its latest Windows update back in May. The issues caused by having the security company's software installed include random freezes, general slowness, video stuttering, blue screen of death (BSOD) crashes and Windows 10 becoming unresponsive.

COMMUNICATIONS AUTHORITY OF KENYA

www.ke-cirt.go.ke