# NATIONAL KE-CIRT/CC CYBERSECURITY UPDATES
# 4th September 2019

COMMUNICATIONS AUTHORITY OF KENYA

## Top Stories

**Source 1: OregonLive (https://www.oregonlive.com/ )**

https://www.oregonlive.com/news/2019/08/122000-providence-health-plan-customers-may-be-affected-by-data-breach.html

*122,000 Providence Health Plan customers may be affected by data breach.* Providence Health Plan is notifying as many as 122,000 health plan members that their insurance information may be at risk. The incident came to light after it was notified by Dominion National of possible unauthorized access. Dominion National and Providence Health Plan have no evidence that any information was viewed, accessed or has been misused.

**Source 2: CISION PR Newswire (https://www.prnewswire.com/ )**

https://www.prnewswire.com/news-releases/notice-of-payment-card-security-incident-300909508.html

*Notice of Payment Card Security Incident.* Russell Stover Chocolates, LLC recently became aware of a data security incident that potentially affected payment cards for some customers. The incident occurred after hackers gained access to Russell Stover's PoS systems through malware. The firm has notified law enforcement agencies about the incident.

**System vulnerabilities**

**Source 1: Security Week (https://www.securityweek.com/ )**

https://www.securityweek.com/zyxel-devices-can-be-hacked-dns-requests-hardcoded-credentials

*Zyxel Devices Can Be Hacked via DNS Requests, Hardcoded Credentials.* Multiple security vulnerabilities have been discovered in various Zyxel devices. The flaws arise due to the use of unauthenticated DNS requests and hardcoded FTP credentials. One of the flaws impacts Zyxel security and networking devices from the USG, UAG, ATP, VPN, and NXC products. Updates to fix the issues have been released at the end of August.

**Source 2: The Hacker News ( https://thehackernews.com/ )**

https://thehackernews.com/2019/08/reverse-rdp-windows-hyper-v.html

*Reverse RDP Attack Also Enables Guest-to-Host Escape in Microsoft Hyper-V.* Microsoft's Hyper-V is a virtualization technology that comes built-in with Windows operating system, enabling users to run multiple operating systems at the same time as virtual machines. It uses Remote Desktop Services to let the host machine connect to a guest virtual machine and share synchronized resources like clipboard data. This means, Hyper-V Manager eventually inherits the Poisoned RDP vulnerability (CVE-2019-0887).

**Source 3: CYWARE( https://cyware.com/ )**

https://cyware.com/news/epignosis-patches-two-vulnerabilities-in-efront-learning-management-system-897c90f2

*Epignosis patches two vulnerabilities in eFront Learning Management System.* Two serious vulnerabilities have been found affecting Epignosis eFront. While the first flaw could allow an attacker to remotely execute code on the victim system, the second flaw opens the victim machine to SQL injections. Epignosis has addressed the issues in eFront version 5.2.13.

**Malware**

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

https://cyware.com/news/newly-discovered-domen-toolkit-leverages-fake-browser-and-software-update-alerts-to-spread-malware-23d72d4c

*Newly discovered Domen toolkit leverages fake browser and software update alerts to spread malware.* A newly discovered Domen social engineering toolkit has been found infecting users' machines with malware. The toolkit is used to display fake browser and software update alerts on compromised sites. The toolkit supports the creation of alerts using 30 different languages and is designed to target both desktop and mobile users.

COMMUNICATIONS AUTHORITY OF KENYA

## DDoS/Botnets

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

https://cyware.com/news/demystifying-ostap-a-new-downloader-for-trickbot-trojan-fdbbaeaa

*Demystifying Ostap, a new downloader for Trickbot Trojan.* Threat actors are increasingly using a new Ostap malware downloader to deliver Trickbot trojan. The malware downloader is distributed through emails as a Microsoft Word 2007 macro-enabled document which contains two components - a VBA macro and JScript. The emails are themed as purchase orders, suggesting that the campaigns are likely intended to target businesses rather than individuals.

## Spam & Phishing

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

https://cyware.com/news/new-phishing-campaign-uses-compromised-sharepoint-sites-to-bypass-secure-email-gateways-3bdf9574

*New phishing campaign uses compromised SharePoint sites to bypass secure email gateways.* Researchers from Cofense have spotted a new phishing campaign that uses SharePoint sites to bypass secure email gateways and target banks with phishing URLs. The emails are sent from compromised accounts, asking the targets to review a legal assessor's proposal via a URL embedded within the message. The URL links to an attacker-controlled SharePoint site.

**Web security**

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

https://cyware.com/news/an-ongoing-malvertising-campaign-is-targeting-millions-of-wordpress-sites-1705da31/

*An ongoing malvertising campaign is targeting millions of WordPress sites.* Cybercriminals have targeted millions of WordPress sites in a massive malvertising campaign. They have managed to pull off the campaign by exploiting the vulnerabilities that reside in some of the most popular plugins such as Bold Page Builder, Bold Designer, Live Chat with Facebook Messenger, and WP Live Chat Support.

## 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-20190904-webex-teams

*Cisco Webex Teams Logging Feature Command Execution Vulnerability.* Due to improper restrictions on software logging features used by the application on Windows operating systems an unauthenticated, remote attacker could execute arbitrary commands on an affected system.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-ind

*Cisco Industrial Network Director Configuration Data Information Disclosure Vulnerability.* Due to improper access restrictions on the web-based management interface an unauthenticated, remote attacker could access sensitive information on an affected device.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-unified-ccx-ssrf

*Cisco Unified Contact Center Express Request Processing Server-Side Request Forgery Vulnerability.* Due to improper validation of user-supplied input on the affected system a remote attacker could bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system.

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-sma-info-dis

*Cisco Content Security Management Appliance Information Disclosure Vulnerability.* Due to incorrect permission controls role  implementation an attacker could gain out-of-scope access to email.

COMMUNICATIONS AUTHORITY OF KENYA

# www.ke-cirt.go.ke