SERIANU CYBER-THREAT ALERT SERVICE

November- December, 2013

Introduction

In this month's SC3 – Serianu CyberThreat Command Center alert service, we highlight a number of high priority vulnerabilities targeting popular technologies employed globally; this includes a variant of an old BankPatch (Multi-Banker) MITM Trojan that was detected in Kenya in late November, Office 365, eRoom, Cisco, MS Office and Zimbra Collaboration server vulnerabilities. We also address software updates available from different vendors.

Contents

CRITICAL : A VARIANT OF AN OLD BANKING MALWARE DETECTED IN KENYA

Discovery: In late November, we detected a variant of an old Man-In-The-Middle banking Trojan known as MultiBanker that steals online banking details from users in the Kenyan cyber-space. MultiBanker was originally very active in Europe between 2007 and 2011 but the variant detected in Kenya is slightly different. MultiBanker (also called Patcher, BankPatch/BankPatcher) is a very targeted banking Trojan. The Trojan has its main component (appconf32.exe, stored in %AppData%) and several plugins which are specific to the installed software (browser) and visited websites. For banks it has special plugins (technically BHOs) that allow exchanging the account number of online banking transactions on the infected machine, effectively stealing the money out of the victim's bank account.

Recommended Remediation:

All users and administrators especially Customers who log Corporate banking websites should adhere to the following basic security "best practices":

1. Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

2. If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

3. Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services (for example, all Windows-based computers should have the current Service Pack installed.)

4. Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

5. Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

6. Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

CRITICAL: SEVERE MS OFFICE 365 TOKEN DISCLOSURE VULNERABILITY

Discovery: A security team recently identified a vulnerability that can allow an attacker to hijack a victim's office 365 authentication token. The attacker can then get access to the organization's Sharepoint Online site, download all the files, modify or manipulate them however they want. All this will be done without the knowledge of the victim.

Affected Systems: Office 365

Exploitation: An individual is compromised when they unknowingly/accidently click on a malicious document or a webpage. The malicious webpage will ask Word for its Office 365 token and he will willingly be provided. The attacker now has access to the Office 365 token and ultimately, he will have access to the organization's SharePoint and SkyDrive Pro documents.

Mitigation: If your organization is currently using SharePoint as a platform to share company documents and files, it's important to ensure that a documents classified as "*highly confidential'* should not be shared and users should be made well aware of the implications of clicking and downloading files from unknown senders.

CRITICAL: ZIMBRA ZERO DAY EXPLOIT

Discovery: Zimbra contains a flaw that may allow a remote attacker to execute arbitrary commands or code. The issue is due to the Local File Inclusion not properly sanitizing user input, specifically directory traversal style attacks (e.g., ../../) supplied to the 'skin' parameter. This may allow an attacker to include a file from the targeted host that contains arbitrary commands or code that will be executed by the vulnerable script. Such attacks are limited due to the script only calling files already on the target host.

In addition, this flaw can potentially be used to disclose the contents of any file on the system accessible by the web server.

This exploit is however only possible if the admin console port 7071 is open.

Affected Systems: Zimbra 7.2.2 & 8.0.2

Mitigation: Upgrade to version 7.2.3 and 8.0.3, or higher, to address this vulnerability. In addition, the vendor has released patches for versions 7.2.2 and 8.0.2.

CRITICAL: WINDOWS AND MS-OFFICE *IN-THE-WILD* EXPLOITS.

Discovery: In November 2013, Microsoft disclosed vulnerability in the graphics code in certain versions of Windows, Office and Lync (popularly used for instant messaging and video conferencing). This attack is specifically targeted towards Microsoft Office users (individuals or corporations) found in the Middle East and South Asia.

Affected systems:

- Windows Vista x86, x64
- Windows Server 2008 x86, x64, Itanium, Server Core
- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010 x86, x64
- Microsoft Office Compatibility Pack
- Microsoft Lync 2010 x86, x64
- Microsoft Lync 2010 Attendee
- Microsoft Lync 2013 x86, x64
- Microsoft Lync Basic 2013 x86, x64

Exploitation: The advanced exploit arrives in a booby-trapped Word document attached to e-mail which if opened or previewed, allows the attacker to exploit the vulnerability using a malformed graphics image embedded in the document. If successful, the attacker can perform remote code executions and attain privileged escalation to the computer system.

In order to achieve code execution, the exploit combines multiple techniques to bypass DEP and ASLR protections using Active X controls to increase memory payload. Once Windows, Office, or Lync programs process the maliciously designed TIFF files, system memory is corrupted in a way that allows the attacker to execute arbitrary code

Mitigation: Microsoft has issued a temporary fix that people can install and use until a permanent patch is available. While it doesn't repair the root cause of the vulnerability, the temporary measure blocks rendering of the graphic format that triggers the bug. Other temporary measures available to Windows and Office users are modifying the Windows registry to prevent TIFF image files from being displayed or *installing version 4.0 of EMET*, short for the Enhanced Mitigation Experience Toolkit.

CRITICAL: TCP PORT ZERO RECONNAISSANCE

Discovery: Researchers from Cisco have alerted customers and the Internet community of a massive spike in TCP source ports zero traffic that started in November 2013. According to a security researcher within Cisco, the traffic experienced that day could have been an attempt to identify network security devices.

Affected Systems: N/A

Exploitation: Different network equipment will respond to this abnormal traffic differently and an attacker may be able to infer which devices a customer is using to protect their network by inspecting this traffic. Similarly different operating systems or even different versions of the same operating system may respond to the use of port zero in different ways. This can help enable the attacker to make a more precise attempt to compromise a network."

Cisco correlated the highest volume of traffic IPs hosted in Netherlands. However, it is important to note that, although reconnaissance may have been conducted from machines in Netherlands, possibilities of the attack being launched from a different set of IPs from another country are highly likely.

Mitigation: This may be the planning stages of an attack, therefore; Cisco advises Network Security teams to block TCP port zero at their firewall and keep an eye on logs for any anomalous or suspicious activities.

CRITICAL: EMC DOCUMENTUM EROOM MULTIPLE CROSS SITE SCRIPTING VULNERABILITIES

Discovery:

Cross-site scripting vulnerabilities could be potentially exploited for conducting malicious scripting attacks in EMC Documentum eRoom (hosted collaborative solution that provides mid-sized businesses with collaboration software in a hosted environment.). The vulnerability could be exploited by getting an authenticated user to click on specially-crafted links that a malicious attacker can embed within an email, web page or other source. This may lead to execution of malicious html requests or scripts in the context of the authenticated user.

Affected Systems: EMC Documentum eRoom.

Mitigation: EMC strongly recommends customers to upgrade to the new version EMC Documentum eRoom version 7.4.4 P11 as soon as possible from Support Zone (https://support.emc.com).

CRITICAL: CISCO TELEPRESENCE VX CLINICAL ASSISTANT ADMINISTRATIVE PASSWORD RESET VULNERABILITY

Discovery: The Cisco TelePresence VX Clinical Assistant is an easy-to-use, high-definition, video collaboration system that is designed for mobility at the point of care. The Cisco TelePresence VX Clinical Assistant is intended to facilitate remote provider/patient and provider/provider consultations.

A vulnerability in the WIL-A module of Cisco TelePresence VX Clinical Assistant could allow an unauthenticated, remote attacker to log in as the *admin* user of the device using a blank password.

Affected Systems: Cisco TelePresence VX Clinical Assistant units running software version 1.2

Exploitation: This vulnerability will reset the password for the "admin" user to a blank password on every reboot whether a password has been set for the user or not. Any passwords configured for the "admin" user remain valid only until the next system reboot, when it will be overwritten by a blank password.

Passwords for other users on the system are not impacted by this vulnerability.

Mitigation: Cisco has released free software updates that address this vulnerability. Customers are advised to ensure that the devices are upgraded to software version 1.21.

CRITICAL: REMOTE CODE EXECUTION IN OPENSSH VULNERABILITY: AES-GCM

Discovery: On November 7, 2013, an OpenSSH developer discovered a memory corruption vulnerability that exists in the post- authentication SSHD process when an AES-GCM Cipher is selected during key exchange. If exploited, this vulnerability might permit code execution with the privileges of the authenticated user and may therefore allow bypassing restricted shell command configurations.

Affected Configurations: OpenSSH 6.2 and OpenSSH 6.3

Mitigation: Disable AES-GCM in the server configuration. The following sshd_config option will disable AES-GCM while leaving other ciphers active. Such as AES128-ctr,AES192-ctr,AES256-ctr,AES128-cbc,3DES-cbc,blowfish-cbc,cast128-cbc, aes192-cbc,aes256-cbc

Because of the popularity of OpenSSH during secure file transfer between servers, we urge system administrators to ensure that they have applied the necessary mitigation strategies. The recent version of OpenSSH, OpenSSH 6.4 contains a fix for this vulnerability. However, users who prefer to continue to use OpenSSH 6.2 or 6.3 may apply the above mentioned patch.

CRITICAL: SAP NETWEAVER GMGAPP SECURITY BYPASS AND INFORMATION DISCLOSURE VULNERABILITY

Discovery: SAP NetWeaver is prone to a security-bypass vulnerability and an information-disclosure vulnerability either locally or remotely. Successful exploits may allow an attacker to obtain sensitive information or bypass certain security restrictions and perform unauthorized actions. This may aid in further attacks. This vulnerability is attributed to:

a) An error within GRMGApp due to the application not properly restricting access can be exploited to e.g. send administrative commands to the Gateway or Message server.
b) An unspecified error within GRMGApp when parsing external XML entities can be exploited to e.g. disclose local files.

Affected Applications: SAP Netweaver 7.30, SAP Netweaver 7.10, SAP Netweaver 7.02, SAP Netweaver 7.01, and SAP Netweaver 7.0.

Exploitation: An attacker can use readily available tools to exploit this vulnerability.

Mitigation: Update SAP Netweaver to its most current available version.

Note: The SAP Netweaver is also reported to have an SQL Injection Vulnerability because it fails to sufficiently sanitize user-supplied input before using it in an SQL query. This vulnerability can be exploited using the web browser. Updates are however available for this vulnerability.

CRITICAL: CRYPTOWARE MALWARE ATTACK

Discovery： This malware encrypts your computer files and demands a huge sum of money as payment to unlock/decrypt them. About 12,000 infected hosts tried connecting to domains associated with Cryptolocker during a one-week period at the end of October. By early November, the malware had infected about 34,000 machines, predominantly in English-speaking countries.

Affected Applications: The malware infects systems running Windows 8, Windows 7, Vista, and XP.

Exploitation: Once a machine becomes infected, Cryptolocker finds and encrypts files located within shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives. If one computer on a network becomes infected, mapped network drives could also become infected. CryptoLocker then connects to the attackers' command and control (C2) server to deposit the asymmetric private encryption key out of the victim's reach. Victim files are encrypted using asymmetric encryption.

The attackers retrieve payments through third-party payment systems like Bitcoin and MoneyPak but some infected users are claiming they paid the attackers and never received a decryption key.

Mitigation: In order to deal with the Cryptolocker infection, follow the guidelines below:

a) Immediately disconnect the infected system from wireless or wired networks. This may prevent the malware from further encrypting any more files on the network.
b) Users who are infected with the malware should consult with a reputable security expert to assist in removing the malware.
c) If possible, change all online account passwords and network passwords after removing the system from the network. Change all system passwords once the malware is removed from the system.
d) Backup your data. A good defense against your data being encrypted by CryptoLocker/Crilock is to have a backup of your files.

SECURITY UPDATES AVAILABLE FOR ADOBE FLASH PLAYER AND COLD FUSION.

Adobe released critical security patches for its ColdFusion web application server and Adobe Flash Player for Mac, Windows and Linux. Adobe AIR and the AIR SDK and Compiler are also being updated.

These updates address vulnerabilities that could cause a crash and potentially allow an attacker to take control of the affected system, dubbed as CVE-2013-5329, CVE-2013-5330. The hotfix for ColdFusion addresses Cross-site scripting (XSS) vulnerability and unauthorized remote read access. Both vulnerabilities were exploited by hackers to steal sensitive data stored on the servers.

Affected Systems:

- Adobe Flash Player 11.9.900.117 and earlier versions for Mac and Windows
- Adobe Flash Player 11.2.202.310 and earlier versions for Linux
- Adobe AIR 3.9.0.1030 and earlier versions for Windows and Macintosh
- ColdFusion versions 10, 9.0.2, 9.0.1 and 9.0 for Windows, Macintosh and Linux,

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com Visit: www.cyberusalama.co.ke for more information on cyber security incidents in Kenya.