SERIANU CYBER-THREAT ALERT SERVICE

January- February, 2014

Introduction

In this January-February 2014 edition of SC3 – Serianu CyberThreat Command Center alert service, we highlight a number of high priority vulnerabilities targeting popular technologies employed globally. Following last year's zero-day vulnerabilities on Windows XP, we highlight on some cases where ATM's operated by Kenyan financial institutions might be susceptible to XP zero-day attacks. In addition, we report on malware that is specifically targeting POS systems and other technologies. We will also focus on the security fixes that have recently been deployed.

Contents

CRITICAL: ATMS FACE DEADLINE TO UPGRADE FROM WINDOWS XP

Discovery: Late last year, 2013, Microsoft announced that they will no longer support Windows XP; this means they will not provide any security patches for vulnerabilities found in the wild. Microsoft has therefore requested all their XP users to upgrade to Windows 7 or a later version of Windows by **July 15. 2015**. This is good news for most companies, who have been struggling to migrate before the earlier deadline of 8th April, 2014. The security updates will ensure that the companies' systems remain secure as they migrate. We have identified cases where a number of ATM's in Kenya still run Windows XP.

Affected Systems: Machines using Windows XP

Globally, the number of ATMs that use Windows XP is estimated to be around 3 million. In the US alone, there are over 420,000 ATMs. Interestingly enough, the hardware components of most of these computers may not be capable of supporting Windows 7. Therefore, the cost of upgrading to Windows 7 may be significantly high depending on whether additional components are required to support the operating system or not.

CRITICAL : MALWARE TARGETING POINT OF SALE SYSTEMS

Discovery: Early this year, the US-Cyber Emergency & Response teams warned retailers against the persistent attacks targeted on the point-of-sale systems. In some circumstances, criminals attach a physical device to the POS system to collect card data, which is referred to as skimming. In other cases, cyber criminals deliver malware which acquires card data as it passes through a POS system and sends the desired data back to the criminal. Once the cybercriminal receives the data, it is often trafficked to other suspects who use the data to create fraudulent credit and debit cards.

Affected systems: POS systems

Exploitation: POS systems are often enabled to access the internet, therefore malicious links or attachments in emails as well as malicious websites can be accessed and malware may subsequently be downloaded by an end user of a POS system. A cyber- criminal gets more value from infecting one POS system as he will yield card data from multiple consumers

One of the largest retailing companies in the U.S, Target Corporation, recently discovered malware on their POS systems that impacted close to 40 million debit and credit card accounts. Fortunately, Target disabled the malicious code and began the process of notifying card processors and payment card networks.

Mitigation: To mitigate against the intensity of loss that such attacks bring about, retailers should ensure that:

- POS systems are isolated from other networks
- Point-to-point encryption is enabled for credit card data protection
- POS system-access to the internet and remote access is restricted
- POS software applications are regularly updated.

NB: Rolling out of the EMV cards will play a great role in mitigating such attacks

CRITICAL: SIEMENS SWITCHES ZERO-DAY FLAWS FOUND

Discovery: Earlier this year, a security researcher discovered a pair of zero-day vulnerabilities in a popular family of Siemens industrial control system switches that could allow an attacker to take over the network devices without a password. Siemens was however notified and patched the flaw soon after. Whether Siemens customers will actually apply the patches or just how quickly they will do so is the big question.

Affected systems: Siemens SCALANCE X-200 switch

Exploitation: According to the researcher, the switches' session id setup was poorly constructed which would allow an attacker to hijack an administrative session on the switch without using any credentials.

The other flaw the researcher came across was where an attacker could gain admin operations to the switch with no credentials required. The attacker could then download any network configuration information, or upload a malware-ridden firmware update etc. If the firmware to the switch is changed, this means that the perpetrator can have access to all traffic to the switch, sniff network credentials and upload malware-laden firmware.

Mitigation: Siemens customers should ensure that apply the patches provided by SIEMENS before an attack occurs.

CRITICAL: VMWARE ESX/ESXI SECURITY ADVISORY

Discovery: In the month of January, VMware released a security advisory VMSA-2013-0016 and involves the ESX (versions 4.0 & 4.1) and ESXi (versions 4.0 through 5.5) products. A vulnerability exists within the products which could allow an unpriviledged vCenter user to arbitrarily have read or write access to files. Removing the "Add Existing Disk" permission or limiting the number of vCenter users with this privilege can reduce the risk of exploitation until updates can be applied.

Affected Systems: VMware ESX/ESXi v4.0 & 4.1

Mitigation: In addition to the applying the patches provided by VMware, the following should also be done:

- In a default vCenter Server installation no unprivileged users or groups are assigned the predefined role "Virtual Machine Power User" or "Resource Pool Administrator".
- Restrict the number of vCenter Server users that have the privilege "Add Existing Disk".

CRITICAL: ORACLE TECHNOLOGY VULNERABILITY SUMMARIES

Discovery: This segment highlights three critical Oracle vulnerabilities with respect to Java, Oracle database and Oracle Solaris.

Oracle Java SE is prone to a remote security vulnerability (CVE-2013-5899) which allows remote attackers to affect confidentiality via unknown vectors related to Deployment. Oracle Database Server on the other hand is prone to a remote security vulnerability in Core RDBMS (CVE-2014-0377). Lastly, Oracle Solaris is prone to a local security vulnerability (CVE-2003-1067). This vulnerability provides administrator access, allows complete confidentiality, integrity, and availability violation, unauthorized disclosure of information and disruption of service.

Affected systems: The Oracle Java SE vulnerability affects Java SE 6u65, Java SE 7u45 respectively. The Oracle Database Server vulnerability affects the Oracle database version 11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1 and the Oracle Solaris vulnerability affects versions 8 and 9.

Exploitation: The CVE-2013-5899 applies to client deployment of Java only. This vulnerability can be exploited only through sandboxed Java Web Start applications and sandboxed Java applets. The Oracle Database Server vulnerability allows remote authenticated users to affect confidentiality via vectors related to SYS tables. The access Vector to exploit this vulnerability is through the Network. The vulnerability identified in Oracle Solaris vulnerability is locally exploitable, with a low complexity and no authentication is requires to facilitate exploit.

It should be noted that the impact of the above named vulnerabilities is that they allow unauthorized disclosure of information.

Mitigation: Java and Oracle customers should ensure that apply the patches provided by Oracle before the servers tuning the defined applications are compromised.

CRITICAL: MICROSOFT VULNERABILITY SUMMARIES

Discovery: Microsoft released vulnerability updates in a bit to tackle vulnerabilities affecting Microsoft Word and Office web apps and the Windows Kernel. The vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2916605) while the vulnerabilities in the windows kernel (2914368) and Windows Kernel-Mode Drivers (2913602) could allow privilege escalation.

Affected systems: The affected systems include Microsoft Word and Office Web Apps vulnerabilities affect Microsoft Office, Microsoft Server Software, the Windows Kernel and Kernel-Mode Drivers on Windows operating systems.

Exploitation: The Microsoft Word and Office Web Apps vulnerabilities could allow remote code execution if a specially crafted file is opened in an affected version of Microsoft Word or other affected Microsoft Office software. An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Windows Kernel vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability

The Windows Kernel-Mode Drivers vulnerability could allow elevation of privilege if a user logs on to a system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability.

Mitigation: Microsoft customers should ensure that apply the updates provided by Microsoft at the earliest time possible and restart the machine**.**

CRITICAL: CISCO SMALL BUSINESS DEVICES VULNERABILITY

Discovery: Cisco has released a new update fix to Cisco WAP4410N Wireless-N Access Point, Cisco WRVS4400N Wireless-N Gigabit Security Router, and the Cisco RVS4000 4-port Gigabit Security Router.

Affected systems: The affected devices are Cisco RVS4000 4-port Gigabit Security Router running firmware version 2.0.3.2 and prior, Cisco WRVS4400N Wireless-N Gigabit Security Router hardware version 1.0 and 1.1 running firmware version 1.1.13 and prior, Cisco WRVS4400N Wireless-N Gigabit Security Router hardware version 2.0 running firmware version 2.0.2.1 and prior and Cisco WAP4410N Wireless-N Access Point running firmware version 2.0.6.1 and prior.

Exploitation: The vulnerability was an attacker can gain root-level access when he/she exploit a service listening on port 32764/tcp. This vulnerability is due to an undocumented test interface in the TCP service listening on port 32764 of the affected device. An attacker could exploit this vulnerability by accessing the affected device from the LAN-side interface and issuing arbitrary commands in the underlying operating system. An exploit could allow the attacker to access user credentials for the administrator account of the device, and read the device configuration. The exploit can also allow the attacker to issue arbitrary commands on the device with escalated privileges.

Mitigation: There are no known workarounds that mitigate these vulnerabilities, however users are advised to their product vendors for assistance with the appropriate course of action as well as update the device to the most recent version available.

CRITICAL: HP-UX Running BIND, Remote Denial of Service (DoS)

Discovery: An unintentional defect in the handling of NSEC3-signed zones can cause BIND to be crashed by a specific set of queries.

Affected systems: The affected Bind versions are 6.0.x -> 9.6-ESV-R10-P1, 9.7 (all versions), 9.8.0 -> 9.8.6-P1, 9.9.0 -> 9.9.4-P1. Development releases 9.6-ESV-R11b1, 9.8.7b1, and 9.9.5b1.

Exploitation: Because of a defect in handling queries for NSEC3-signed zones, BIND can crash with an "INSIST" failure in name.c when processing queries possessing certain properties. By exploiting this defect an attacker deliberately constructing a query with the right properties could achieve denial of service against an authoritative nameserver serving NSEC3-signed zones.

Mitigation: Upgrade to the patched release most closely related to your current version of BIND.

CRITICAL: OpenSSL Vulnerability

Discovery: This vulnerability is where the client NULL dereference crashes due to malformed handshake packets.

Affected systems: **O**penSSL 1.0.1 and before 1.0

Exploitation: The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.

Mitigation: Upgrade to the most current version of Open SSL.

CRITICAL: IBM Tivoli Vunlerability

Discovery: The Tivoli Federated Identity Manager Business Gateway 6.2.2 Risk Based Access feature can be configured to require that a user provide a One Time Password (OTP) token before being able to perform a sensitive transaction. As the name implies, these tokens should only be valid for a single use. If a malicious user or system were to obtain such a token and attempt to use it to authenticate after it had already been used, such replay should be denied by TFIMBG. The discovered vulnerability allows OTP tokens to be reused under special condition

Affected systems: Tivoli Federated Identity Manager 6.2.2

Exploitation: The attack does not require local network access, but it does require authentication and highly specialized knowledge and techniques. An exploit would not impact the confidentiality of information or the availability of the system, but the integrity of data could be compromised.

Mitigation: Upgrade to the most current version of Tivoli Federated Identity Manager 6.2.2. The patching and upgrade instructions are provided on the vendor website.

CRITICAL: Cisco Video Surveillance 5000 Series HD IP Dome Cameras Vulnerability

Discovery: The Cisco Video Surveillance 5000 Series HD IP Dome Cameras is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the Web interface

Affected systems: Cisco Video Surveillance 5000 Series HD IP Dome Camera

Exploitation: A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

Mitigation: Upgrade to the most recent software version available for the device.

CRITICAL: Multiple MySQL Vulnerabilties

Discovery: Several issues have been discovered in the MySQL database server. The CVE IDs are CVE-2013-5891 CVE-2013-5908 CVE-2014-0386 CVE-2014-0393 CVE-2014-0401 CVE-2014-0402 CVE-2014-0412 CVE-2014-0420 and CVE-2014-0437.

Affected systems: The affected Oracle Database server version is MySQL 5.5

Exploitation: A buffer overflow flaw was found in the way the MySQL command line client tool (mysql) processed excessively long version strings. If a user connected to a malicious MySQL server via the mysql client, the server could use this flaw to crash the mysql client or, potentially, execute arbitrary code as the user running the mysql client. The multiple vulnerabilities can be exploited remotely and a successful attack results in Denial of Service (DOS) or remote code execution.

Mitigation: Upgrade your mysql-5.5 packages to the most recent version available.

CRITICAL: Adobe Shockwave Player Vulnerabilities

Discovery: Shockwave Player is needed to display online content like games, product demonstrations, e-learning courses and simulations created with Adobe's Director Software. Adobe has released a security update for Adobe Shockwave Player 12.0.7.148 and earlier versions on the Windows and Macintosh operating systems.

Affected systems: The affected application is Adobe Shockwave Player 12.0.7.148 and earlier versions for Windows and Macintosh.

Exploitation: This update addresses critical vulnerabilities that could potentially allow an attacker to remotely take control of the affected system. Shockwave Player installs a plug-in in Web browsers which means it can be attacked with drive-by download exploits loaded from maliciously crafted or infected websites.

Mitigation: We recommend users of Adobe Shockwave Player 12.0.7.148 and earlier versions to update to the newest version 12.0.9.149. The update is available on the Adobe website.

CRITICAL: Apple iOS SSL Vulnerability

Discovery: Apple has issued an urgent fix for vulnerability in its SSL (Secure Sockets Layer) code, used to create secure connections to websites over Wi-Fi or other connections, for its iPhone, iPad and iPod Touch devices. This vulnerability allows almost any attempt to verify a certificate on a website to succeed - whether or not the certificate's signature was valid. It would only give an error if the certificate itself was.

Affected systems: The affected devices are iOS 6 and iOS 7. This vulnerability also affects Mac computers running Mac OSX.

Exploitation: This vulnerability could allow your connections to secure sites to be spied on and/or your login details captured as the vulnerability affects the SSL/TLS encrypted connection to remote sites. In other words, anything you send across the Internet could be intercepted or changed.

Mitigation: In order to mitigate the vulnerability in Mac OSX, update your device to version OSX 10.9.2. If you use an iPhone, iPad or iPod Touch, update its operating software. For devices using iOS 7, update to iOS 7.0.6 and for devices on iOS 6 which can't be updated to iOS 7 (the iPhone 3GS or iPod Touch 4G), update to 6.1.6.

About the Serianu Cyber Threat Alert ServiceFor 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.