SERIANU CYBER-THREAT ALERT SERVICE

March - April, 2014

Introduction

In this month's edition of SC3 – Serianu CyberThreat Command Center alert service, we highlight a critical OpenSSL vulnerability that requires urgent response from its users. We also discuss emergent and persistent attacks targeting financial institution's teller machines and popularly used technologies such as Adobe, Windows 7, Cisco Routers among others. We will also focus on the security fixes that have recently been deployed.

Contents

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.

VERY CRITICAL: ZERO DAY ATTACK TARGETS INTERNET EXPLORER

Discovery: Early this week, Microsoft released a Security Advisory which impacts Internet Explorer versions 6 through 11, taking advantage of a vulnerability in Flash.

Affected Systems: Internet Explorer 6 - 11

Exploitation: The Microsoft advisory notes that "The vulnerability is a remote code execution vulnerability. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website."

Mitigation: Microsoft has not yet issued a stopgap "Fix-It" solution for this vulnerability. For now, it is urging IE users to download and install its Enhanced Mitigation Experience Toolkit (EMET), a free tool that can help beef up security on Windows. Microsoft notes that EMET 3.0 doesn't mitigate this attack, and that affected users should instead rely on EMET 4.1. I've reviewed the basics of EMET here.

Remediation steps

- Disable Flash. Note that IE 10 and later on Windows 8 do include Flash. But you can still disable it. This is an Internet Explorer vulnerability but Flash is needed to exploit it and bypass some of the protection techniques implemented in newer versions of IE/Windows.
- Enable the Internet Explorer "Enhanced Protection Mode" (EPM) which became available in Internet Explorer 10.

CRITICAL: MAJOR OPENSSL 'HEARTBLEED' VULNERABILITY

Discovery: A major OpenSSL bug was recently discovered by security researchers. The Heartbleed Bug is a serious vulnerability and allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

Affected Systems: OpenSSL cryptographic software library

Exploitation: The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Mitigation: Due to the SEVERITY of the bug, we urge users of OpenSSL to take immediate action. Please email us on info@serianu.com for assistance in fixing this vulnerability.

CRITICAL: U.S SECRET SERVICE WARNS OF CYBER ATTACKS TARGETING ATM

Discovery: Earlier this month, the U.S Secret Service warned about the threat of rising cyber-attacks on bank websites and cash machines, urging the industry to put proper measures in place to guard against fraud.

Affected Systems: Bank ATMs

Exploitation: Cyber criminals are able to withdraw large amounts of money from ATMs. Recently, the criminals stole up to 40 million dollars from 12 customer accounts.

To be able to perpetrate the attack, cyber criminals install malicious software on a bank's computers through phishing emails, and then hack into control panels to raise limits on how much a cash machine can dispense. Once this is successful, they use stolen bank cards to withdraw money, usually over the weekend. These operations can be accompanied by a denial-of-service attack, in

which a bank's website is flooded with information requests so that it slows down or completely stops working for clients with legitimate requests.

Mitigation: Currently, the best mitigation would be migration to EMV cards, this reduces the chances of user's ATM card from being copied.

CRITICAL: JOOMLA CRITICAL SQL VULNERABILITY PATCH

Discovery: A critical vulnerability was found in Joomla. Affected by this issue is an unknown function of the file */index.php/weblinks-categories* upon manipulation of the argument id with pre-defined input results in SQL injection vulnerability. This vulnerability impacts confidentiality, integrity, and availability.

Affected Applications: Joomla version 3.2.1

Exploitation: This vulnerability can be readily exploited. An attacker can readily download the exploit and attack Any server that appears vulnerable.

Mitigation: Currently, we do not have any information on possible countermeasures. However, possible controls could be the replacement of affected object with an alternative product.

CRITICAL: 300,000-PLUS WIRELESS ROUTERS HIJACKED

Discovery: Team-Cymru researchers uncovered a mass compromise of home and small-office wireless routers, being used to make malicious configuration changes to more than 300,000 devices made by D-Link, Micronet, Tenda, TP-Link, and other well-known brands.
Affected systems: TP-Link TD-8840t is an ADSL2+ Ethernet/USB Modem Router which works with a 24-Mbps downstream connection.

Exploitation: The attacker modifies the victim's router DNS settings to resolve to a malicious DNS that consists of malicious specially crafted webpages. If the current user admin visits this page his password will be reset to blank and the attacker can login with the username admin and password (blank).

Mitigation:

- Check the router regularly to ensure DNS settings that have been changed
- Ensure the device is running the latest-available version of the firmware and disable remote administration capabilities if they're not needed. In the event they are needed, users should limit the remote IP addresses that can access the router.
- Lastly, it can be helpful to disable a router's Web interface in favor of a command line since the interfaces are often susceptible to cross-site request forgeries and other types of attacks that target Web-programming weaknesses.

CRITICAL: SAMSUNG GALAXY DEVICES - ANDROID BACKDOOR

Discovery: Researchers found that the radio modems on some Samsung devices will execute remote file system (RFS) commands. It was discovered that the proprietary program running on the applications processor actually implements a back door that lets the modem perform remote read, write, and delete files on the phone's storage. On several phone models, this program runs with sufficient rights to access and modify the user's personal data

Affected Devices: The affected devices are the Nexus S, Galaxy S, Galaxy S 2, Galaxy Note, Galaxy Nexus, Galaxy Tab 2 7.0, Galaxy Tab 2 10.1, Galaxy S 3, and Galaxy Note 2.

Exploitation: Attackers can remotely exploit a software-based backdoor to steal files and location data or secretly activate a microphone or camera.

Mitigation: Android users are advised to update to the most current software version available for their respective devices.

CRITICAL: CISCO ROUTER PASSWORD DISCLOSURE VULNERABILITY

Discovery: The web management interface on the Cisco RV110W firewall with firmware 1.2.0.9 and earlier, RV215W router with firmware 1.1.0.5 and earlier, and CVR100W router with firmware 1.0.1.19 and earlier does not prevent replaying of modified authentication requests, which allows remote attackers to obtain administrative access by leveraging the ability to intercept requests.

Affected Devices: This vulnerability affects the following versions of cisco devices: Cisco RV110W Wireless-N VPN Firewall running firmware versions 1.2.0.9 and prior, Cisco RV215W Wireless-N VPN Router running firmware versions 1.1.0.5 and prior and Cisco CVR100W Wireless-N VPN Router running firmware versions 1.0.1.19 and prior.

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.

Exploitation: An attacker can bypass the login page of the router just manipulating the POST data in the router administration page and gain access like an administrator.

Mitigation: Update the router with the most current firmware available.

CRITICAL: ADOBE SHOCKWAVE PLAYER - MEMORY CORRUPTION VULNERABILITY

Discovery: Adobe Shockwave Player before 12.1.0.150 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

Affected applications: This vulnerability affects Adobe Shockwave Player 12.0.9.149 and earlier versions on the Windows and Macintosh operating systems.

Exploitation: An exploit against this vulnerability would potentially allow an attacker to remotely take control of the affected system.

Mitigation: It is recommended that users of Adobe Shockwave Player 12.0.9.149 and earlier versions update to Adobe Shockwave Player 12.1.0.150 using the instructions provided on their website.

CRITICAL: MULTIPLE WINDOWS OS VULNERABILITIES

Discovery: This bulletin covers two CVEs that affect the Windows Kernel Mode Driver, Win32k.sys. CVE-2014-0300 is privilege elevation vulnerability. If an attacker has a valid logged-in session they can execute a malicious application that will give them full administrative rights to the system. CVE-2014-0323 can allow improper disclosure of objects in memory.

Affected applications: This vulnerability affects Windows XP, Vista, 7, 8, 8.1, RT as well as Windows Server 2003, 2008, 2012

Exploitation: This vulnerability could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. However, for this to happen, the attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities.

Mitigation: Permit local access for trusted individuals only. Where possible, use restricted environments and restricted shells. To exploit this vulnerability, an attacker requires local access to an affected computer therefore grant local access for trusted and accountable users only.
Windows users are advised to update to the most recent security updated available for the platform.

The security update addresses the vulnerabilities by correcting the way that the Windows kernel-mode driver handles objects in memory.

CRITICAL: MULTIPLE INTERNET EXPLORER VULNERABILITIES

Discovery: These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. The multiple vulnerabilities are reported under the following vulnerability candidates i.e. CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, CVE-2014-0322 and CVE-2014-0324.

Affected applications: The vulnerable applications are Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 on affected Windows clients, and Moderate for Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 on affected Windows servers.

Exploitation: This vulnerability could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these 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.

Mitigation: Internet explorer users are advised to install and apply the most recent security updates available to their systems. This security update addresses the vulnerabilities by modifying the way that Internet Explorer handles objects in memory.

CRITICAL: EMERGENT NTP AMPLIFICATION ATTACKS

Discovery: A Network Time Protocol (NTP) Amplification attack is an emerging form of Distributed Denial of Service (DDoS) that relies on the use of publically accessible NTP servers to overwhelm a victim system with UDP traffic.

The NTP service supports a monitoring service that allows administrators to query the server for traffic counts of connected clients. This information is provided via the “monlist” command. The basic attack technique consists of an attacker sending a "get monlist" request to a vulnerable NTP server, with the source address spoofed to be the victim’s address.

Affected device: NTP servers.

Exploitation: The attack relies on the exploitation of the 'monlist' feature of NTP, as described in CVE-2013-5211, which is enabled by default on older NTP-capable devices. This command causes a list of the last 600 IP addresses which connected to the NTP server to be sent to the victim. Due to the spoofed source address, when the NTP server sends the response it is sent instead to the victim. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks.

Mitigation: As all versions of ntpd prior to 4.2.7 are vulnerable by default, the simplest recommended course of action is to upgrade all versions of ntpd that are publically accessible to at least 4.2.7. However, in cases where it is not possible to upgrade the version of the service, it is possible to disable the monitor functionality in earlier versions of the software.

To disable “monlist” functionality on a public-facing NTP server that cannot be updated to 4.2.7, add the “noquery” directive to the “restrict default” line in the system’s ntp.conf, as shown below:

- restrict default kod nomodify notrap nopeer noquery
- restrict -6 default kod nomodify notrap nopeer noquery

ADOBE READER VULNERABILITY

Discovery: A critical vulnerability was found in Adobe Reader 11.0.06. This affects an unknown function of the component *Sandbox*.

Affected applications: This vulnerability is present in Adobe Reader version 11.0.6

Exploitation: The manipulation with an unknown input leads to a privilege escalation vulnerability in the application. This vulnerability results in the compromise of confidentiality, integrity, and availability while interacting with the compromised application.

Mitigation: At the time of development of this publication, we are not aware of any vendor-supplied patches to mitigate this vulnerability.