SERIANU CYBER THREAT ALERT SERVICE

April 11, 2013

Introduction

The Serianu Cyber Threat Alerts provide monthly summaries of new vulnerabilities and timely information about current security issues, vulnerabilities, and exploits. The April 2013 alert includes vulnerabilities that affect different constituents. Specifically organisations that rely on Point of Sale systems, CISCO Linksys WiFi Routers and Postgresql database system.

Contents

CRITICAL: New Malware harvests Card Data on POS systems and ATMs

Discovery:

Security researchers earlier this month discovered malware dubbed “Dump Memory Grabber” that targets POS systems and ATMs to steal debit and credit card information from customers. According to the researcher’s, the malware has already been used by modern cybercriminals to steal sensitive information from credit and debit card customers using US banks including Chase, Citibank and Capital One. Most of them were organized with the help of insiders within the Banks, who have access to the POS to maintain or update its software locally. This is not the first time attacks have been directed at bank ATMs. Late last year, one of Kenya’s leading banks admitted to having been attacked by fraudsters through a process called skimming – this involves moldings placed on top of the ATM card slots and keypads that log information from unsuspecting customers. Evidently, unlike skimming, dump memory

grabber is installed directly into POS hardware and ATMs either through USB drives or directly via the web.

In addition, in their recent Report, McAfee pointed out that 38% of the systems used in the retail sector today are running DOS or a legacy version of Windows. Therefore, infrequently updated POS systems give malicious users opportunities to attack.

Affected systems: The attacks target bank ATMs and POS systems with accessible ports and/or direct connections to the web.

Exploitation: Successful exploitation of this malware is achieved by physically inserting a malicious USB drive or via the Web if the target system is directly connected to the Internet. The malware adds itself to the systems registry and automatically runs whenever the systems boot up and searches memory for sensitive data such as primary account number, first and last name, and expiration date. Financial fraudsters will then use this information (transmitted to the remote server via FTP) to clone physical credit and debit cards.

Mitigation: Currently, this malware is still under investigation, however; Serianu recommends that card consumers take precaution when using ATMs and POS machines.

CRITICAL: CISCO IOS and IOS XE devices Vulnerable to Brute-force Attacks

Discovery: Networking vendor Cisco Systems Inc. has issued a security advisory regarding password issues discovered in a limited number of its IOS- and IOS XE-based networking devices that could create conditions for successful brute-force attacks. These devices use the new Type-4 algorithm as an effort to protect routers and switches from brute force attacks. According to Cisco "the Type 4 algorithm was designed to be a stronger alternative to the existing Type 5 and Type 7 algorithms to increase the resiliency of passwords used for the *enable secret password* and *username secret passwor*d commands against brute-force attacks." Unfortunately, this Type 4 does not use random data as additional input to the password (salting) along with a cryptographic hash hence the weakness.

Affected Systems: IOS and IOS XE devices with support for Type 4 passwords

Exploitation: Because a single iteration of the SHA-256 cryptographic hash function is used instead of the intended Password-Based Key Derivation Function version 2 (PBKDF2) in the Type 4 password hash, a malicious user may exploit this vulnerability to decode passwords through exhaustive effort (brute-force attack.)

Mitigation: Cisco recommends that its customers running a Cisco IOS or Cisco IOS XE release with support for Type 4 passwords and currently using Type 4 passwords on their device configuration may want to replace those Type 4 passwords with Type 5 passwords.

CRITICAL: Cisco Linksys Wi-Fi Router Exposed

Discovery: A security expert recently discovered that Cisco Linksys Wi-Fi Router exposes users to a variety of exploits that allow remote attackers to take full control of the device. The most severe of the vulnerabilities is a cross-site request forgery weakness in the browser-based administration panel and also, the routers do not require the current password to be entered when the passcode is changed.

Affected Systems: Linksys EA2700 Manager running the classic firmware

Exploitation: Attackers can successfully exploit the two vulnerabilities mentioned above and take full control of the router by luring anyone connected to it to a booby-trapped website. Malicious JavaScript in the end-user's browser resets the password and turns on remote management capabilities. The attacker can then gain administrative privileges over the device enabling him to perform unscrupulous changes such as installing a version of the device firmware that contains a backdoor and changing settings to use malicious domain name lookup servers.

Mitigation: Users of the Linksys Wi-Fi router are urged to upgrade their firmware to the current Linksys Smart Wi-Fi Firmware

PostgreSQL Patches Critical Vulnerability

Discovery: Earlier this month, Postgresql team released patch updates for a vulnerability that allowed an attacker to corrupt an entire database and/or escalate privileges and in some cases execute commands of his choice (arbitrary code).

Owing to the popularity of this open source object-relational database system, many users may be vulnerable hence the need to apply the patch.

Affected Systems: PostgreSQL versions 9.0, 9.1 and 9.2 running on a public cloud or those with unrestricted access to their network ports.

Exploitation: An authenticated attacker may use this vulnerability to cause PostgreSQL error messages to be appended to targeted files in the PostgreSQL data directory on the server. Files corrupted in this way may cause the database server to crash, and to refuse to restart i.e. Cause a persistent denial-service-attack on the vulnerable server.
In the event that an attacker has a legitimate login on the database server, and the server is configured such that this user name and the database name are identical (e.g. user *web*, database *web*), then this vulnerability may be used to temporarily set one configuration variable with the privileges of the SuperUser i.e. configuration setting privilege escalation.

Mitigation: It is important that all PostgreSQL users apply updates provided by the PostgreSQL team. Also, it is imperative that users ensure that PostgreSQL is not open to connections from untrusted networks. An internal audit would suffice to ascertain that all logins require proper credentials, and that the only logins which exist are legitimate and in current use.

Scribd Compromised; 1 Million Users Exposed

Discovery: The world's largest document sharing site Scribd was hacked earlier this week. Up to one percent of its 100 million users' passwords were compromised due to being stored with an outdated hashing algorithm, Secure Hash Algorithm-1 (SHA-1) and have been salted. The good news however, hackers were not able to crack any of the passwords to get unauthorized access to users' accounts. Compromised users have been requested by Scribd to change their passwords as soon as possible via e-mail after having them reset.

Samsung Android phone Vulnerabilities

Discovery: Security researchers discovered six (6) vulnerabilities in Samsung mobile phones with Android operating systems. Two of the vulnerabilities could allow an attacker to install highly privileged applications without requiring any action on the part of the user. A third issue allows an attacker to take almost any action on a phone, while the fourth allows an attacker to send a Short Message Service

(SMS) communication. A variety of other issues could allow a malicious program to change different settings on the victim's phone.

Affected systems: Galaxy Tab and newer devices such as Galaxy S3

Mitigation*:* Samsung is yet to come up with a patch update

Microsoft Releases Nine Bulletins This Week

On Tuesday, April 9, Microsoft issued nine security bulletins to address vulnerabilities in a number of its products, including Windows, Internet Explorer, Office, and Microsoft Server Software. Below, Serianu provides a summary of the patches for the severe vulnerabilities:

Vulnerability	Description
Critical: Remote Code Execution on MS Windows and Internet Explorer	This security update resolves two privately reported vulnerabilities in Internet Explorer. These vulnerabilities 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.
Important: Information Disclosure in SharePoint Workspace	This security update resolves a publicly disclosed vulnerability in Microsoft SharePoint Server. The vulnerability could allow information disclosure if an attacker determined the address or location of a specific SharePoint list and gained access to the SharePoint site where the list is maintained. The attacker would need to be able to satisfy the SharePoint site's authentication requests to exploit this vulnerability

Important : Elevation of Privilege in Windows Kernel	This security update resolves two privately reported vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker must have valid logon credentials and be able to log on locally to exploit these vulnerabilities.
Important : Denial of Service in Active Directory	This security update resolves a privately reported vulnerability in Active Directory. The vulnerability could allow denial of service if an attacker sends a specially crafted query to the Lightweight Directory Access Protocol (LDAP) service.

Microsoft users are requested to apply the updates immediately.

New Firefox 20 Improves Private Browsing

Mozilla has released Firefox 20, which fixes 13 security issues and makes private browsing easier. Five of the vulnerabilities are deemed critical and could be exploited to run malicious code or install software without user interaction. Firefox 20 also allows users to switch browser privacy status without closing or restarting Firefox; users can instead open a private window while the regular window is open. This version also offers a download panel for easier tracking of files that have been downloaded using Firefox. Firefox should update automatically for users with existing versions of the browser on their computers. Firefox 20 is available for Windows, Mac OS X, and Linux.

About the Serianu Cyber Threat Alert Service

For more detailed and customized vulnerability management service, e-mail us at info@serianu.com