Patching von Sicherheitslücken für Mac OS X

Apple OS X bietet zwar bekanntermaßen größere Sicherheit als andere Betriebssysteme, ist aber dennoch hin und wieder für Angriffe anfällig. Unternehmen und IT-Abteilungen können sich jedoch auf eine schnelle Reaktion von Apple

auf derartige Angriffe verlassen und darauf, dass mit der Casper Suite Patches einfach implementiert und größere Sicherheitsprobleme zeitnah minimiert werden können.

Weiter unten finden Sie einige aktuelle OS X -Sicherheitsangriffe und Informationen dazu, wie diese von Apple und der Casper Suite bewältigt wurden.

Heartbleed Bug

Gemeldet: April 2014

Bedrohung:

Die Verschlüsselungsschlüssel von OpenSSL (die Grundlage für sicheren Datenverkehr im Internet) wurde kompromittiert, sodass Angreifer sensible Daten abrufen konnten.

Lösung:

JAMF Software hat JAMF Nation und JAMF Cloud automatisch für Kunden aktualisiert. IT-Administratoren, die JDS für Linux ausführen, mussten die neueste Version installieren.

NVD-Auflistung: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/discussion.html?id=10317

Bash Bug „Shellshock“

Gemeldet: September 2014

Bedrohung:

Eine Sicherheitslücke in der Befehlszeile von OS X (insbesondere Bash) hat es Remote-Angreifern ermöglicht, eine Verbindung mit anfälligen Computern herzustellen und Befehle auszuführen.

Lösung:

IT-Administratoren, die die Casper Suite verwenden, haben eine Richtlinie erstellt, um das offizielle OS X-Bash-Update 1.0 von Apple zu verteilen: https://support.apple.com/HT201393. Sie haben außerdem einen Bericht ausgeführt, um sicherzustellen, dass der Patch auf alle Macs eingespielt wurde.

NVD Listing: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/discussion.html?id=11914

POODLE

Gemeldet: Oktober 2014

Bedrohung:

SSL (ein Protokoll für sicheren Internetdatenverkehr) wurde für einen „Man-in-the-Middle“-Angriff anfällig, bei dem ein Angreifer Daten zwischen zwei Punkten abfangen und die Informationen entschlüsseln konnte.

Lösung:

IT-Administratoren, die die Casper Suite verwenden, haben eine Richtlinie erstellt, um das offizielle Apple-Sicherheitsupdate 2014-005 zu verteilen: https://support.apple.com/de-de/HT203107. Sie haben außerdem einen Bericht ausgeführt, um sicherzustellen, dass der Patch auf alle Macs eingespielt wurde. Darüber hinaus hatten Casper Suite-Benutzer die Option, ein manuelles Upgrade auf 9.61 vorzunehmen: http://www.jamfsoftware.com/resources/casper-suite-release-notes-version-9-61/

NVD Listing: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/discussion.html?id=12151

Thunderstrike

Gemeldet: Januar 2015

Bedrohung:

Thunderstrike bezieht sich auf einen Angriff auf die Firmware (die grundlegende Software eines Computers) über den Thunderbolt-Hardwareport. Dadurch konnten Angreifer die vollständige Kontrolle über einen Mac und dessen Daten erlangen.

Lösung:

IT-Administratoren, die die Casper Suite verwenden, haben eine Richtlinie erstellt, um das Update 10.10.2 in allen Macs zu verteilen: https://support.apple.com/de-de/HT204942. Sie haben außerdem einen Bericht ausgeführt, um sicherzustellen, dass der Patch auf alle Macs eingespielt wurde.

NVD Listing: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3678
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/discussion.html?id=15363

FREAK-SSL/TLS-Sicherheitslücke

Gemeldet: März 2015

Bedrohung:

Ein Fehler in SSL ermöglichte es einem Angreifer, sicheren Internetdatenverkehr abzufangen und eine schwache Verschlüsselung durchzusetzen, sodass der Angreifer letztendlich Daten stehlen konnte. Websites und Browser waren für diesen Angriff anfällig.

Lösung:

IT-Administratoren, die die Casper Suite verwenden, haben eine Richtlinie erstellt, um das Sicherheitsupdate in allen Macs zu verteilen: https://support.apple.com/de-de/HT204413. Sie haben außerdem einen Bericht ausgeführt, um sicherzustellen, dass der Patch auf alle Macs eingespielt wurde.

NVD Listing: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1067
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/discussion.html?id=13661

Logjam-Angriff

Gemeldet: Mai 2015

Bedrohung:

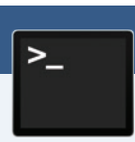
Transport Layer Security (TLS) ist ein Protokoll, das Datenschutz zwischen miteinander kommunizierenden Anwendungen und deren Benutzern im Internet sicherstellt. Der Logjam-Angriff nutzte eine Sicherheitslücke in TLS aus, über die ein Angreifer Sicherheitsmaßnahmen umgehen konnte

Lösung:

IT-Administratoren, die die Casper Suite verwenden, haben eine Richtlinie erstellt, um das Update 10.10.4 oder Sicherheitsupdate 2015-005 in allen Macs zu verteilen: https://support.apple.com/HT204942. Sie haben außerdem einen Bericht ausgeführt, um sicherzustellen, dass der Patch auf alle Macs eingespielt wurde.

NVD Listing: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/article.html?id=384

DYLD_PRINT_TO_FILE



Gemeldet: August 2015

Bedrohung:

Ein Fehler in DYLD (ein Programm auf niedriger Ebene, das die Ausführung des Betriebssystems unterstützt) erteilte Nicht-Administratoren Administratorberechtigungen. Damit konnten Angreifer die vollständige Remote-Kontrolle über einen Mac erlangen.

Lösung:

IT-Administratoren, die die Casper Suite verwenden, haben eine Richtlinie erstellt, um das Sicherheitsupdate in allen Macs zu verteilen: http://support.apple.com/de-de/HT205031.

Sie haben außerdem einen Bericht ausgeführt, um sicherzustellen, dass der Patch auf alle Macs eingespielt wurde.

NVD Listing: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3760
JAMF Nation Thread: https://jamfnation.jamfsoftware.com/discussion.html?id=16563

Bei jeder Computerplattform kommt es zu Sicherheitslücken. Mit Apple OS unter Management durch die Casper Suite kommen sie aber viel seltener vor, sind sehr viel weniger schwerwiegend und werden erheblich schneller behoben.

JAMF software

Um weitere Informationen zu erhalten, senden Sie eine E-Mail an germany@jamfsoftware.com oder rufen Sie uns unter +49 699 675 97 37 an.

www.jamfsoftware.com