jamf

WHITE PAPER

Patching Mac OS X Security Vulnerabilites

While it’s well argued that Apple’s OS X is more secure than other operating systems, it’s still vulnerable to the occasional bug launched by attackers.

What should be reassuring for organizations and IT is Apple’s quick response to such attacks and the Jamf Pro’s ability to easily implement patches and minimize larger security issues in a timely manner.

On the following pages are some recent OS X security attacks and how they were managed by Apple and the Jamf Pro.

To see how Jamf Pro can facilitate personalized learning in your environment, visit: **www.jamf.com/products/Jamf-Pro**

Thunderstrike

Date Reported: January 2015

Threat:

Thunderstrike refers to the attacking of the firmware—a computers most basic software—via the Thunderbolt hardware port. This gave an attacker full control of a Mac and its data.

Solution:

IT admins using the Jamf Pro created a policy to distribute the 10.10.2 Update to all Macs: https://support.apple.com/HT204942. They also ran a report to ensure all Macs were patched.

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 Vulnerability

Date Reported: March 2015

Threat:

A bug in SSL allowed an attacker to intercept secure internet traffic and forced them to use a weak encryption that eventually allowed the attacker to steal data. Websites and browsers were vulnerable to this attack.

Solution:

IT admins using the Jamf Pro created a policy to distribute the Security Update to all Macs: https://support.apple.com/HT204413. They also ran a report to ensure all Macs were patched.

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 Attack

Date Reported: May 2015

Threat:

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. The Logjam attack exploited a vulnerability in TLS that gave an attacker the ability to bypass security measures.

Solution:

IT admins using the Jamf Pro created a policy to distribute the 10.10.4 Update or Security Update 2015-005 to all Macs: https://support.apple.com/HT204942. They also ran a report to ensure all Macs were patched.

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

Date Reported: August 2015

Threat:

A bug in DYLD—a low level program that helps the operating system run—was found to give admin-level privileges to non admins allowing attackers to take full control of a Mac remotely.

Solution:

IT admins using the Jamf Pro created a policy to distribute the Security Update to all Macs: https://support.apple.com/en-us/HT205031. They also ran a report to ensure all Macs were patched.

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

Conclusion

Vulnerabilities are going to happen with any computer platform. But with Apple OS—managed by the Jamf Pro—they're going to happen much less often, be much less severe, and be resolved much more quickly.

jamf

www.jamf.com

To learn more about how Jamf Pro can make an impact on your Mac and iOS management, visit **jamf.com/products/Jamf-Pro**.