Newsletter – Cyber security

Issue – May 2018

Red Hat Linux DHCP Client Found Vulnerable to Command Injection Attacks

Security researcher have discovered a critical remote command injection vulnerability in the DHCP client implementation of Red Hat Linux and its derivatives like Fedora operating system.

The vulnerability, tracked as CVE-2018-1111, could allow attackers to execute arbitrary commands with root privileges on targeted systems. Whenever your system joins a network, it's the DHCP client application which allows your system to automatically receive network configuration parameters, such as an IP address and DNS servers, from the DHCP (Dynamic Host Control Protocol) server.

Adobe Releases Critical Security Updates for Acrobat, Reader and Photoshop

Adobe has just released new versions of its Acrobat DC, Reader and Photoshop CC for Windows and macOS users that patch 48 vulnerabilities in its software.

A total of 47 vulnerabilities affect Adobe Acrobat and Reader applications, and one critical remote code execution flaw has been patched in Adobe Photoshop CC.

WordPress Update Breaks Automatic Update Feature

WordPress version 4.9.3 was released earlier this week with patches for a total 34 vulnerabilities, but unfortunately, the new version broke the automatic update mechanism for millions of WordPress websites.

WordPress team has now issued a new maintenance update, WordPress 4.9.4, to patch this severe bug, which WordPress admins have to install manually.

Apple's iBoot Source Code for iPhone leaked on GitHub

Apple source code for a core component of iPhone's operating system has purportedly been leaked on GitHub, which could allow hackers and researchers to discover currently unknown zero-day vulnerabilities to develop persistent malware and iPhone jailbreaks.

The source code appears to be for iBoot—the critical part of the iOS operating system that's responsible for all security checks and ensures a trusted version of iOS is loaded.

Contact

chahira.miled@keypoint.com
T: +973 1720 0025

This newsletter is intended to provide customers with general information gathered from different sources that are generally believed to be reliable. Keypoint Solutions W.L.L. does not guarantee the accuracy or completeness of the information and does not undertake to keep it up to date. Use of the information made available in this newsletter is at the customer's own risk and Keypoint, its subsidiaries and affiliates expressly disclaim any liability for any errors or omissions reflected herein. The information in this newsletter does not constitute legal or tax advice.