

Newsletter – Cyber security

Issue 17-011 – February 2018



Microsoft missing major Skype patches

A serious vulnerability has been discovered in Microsoft-owned most popular free web messaging and voice calling service Skype that could potentially allow attackers to gain full control of the host machine by granting system-level privileges to a local, unprivileged user.

It's not because the flaw cannot be fixed, but because fixing the vulnerability requires a significant software rewrite, which indicates that the company will need to issue an all-new version of Skype rather than just a patch.

PyeongChang 2018 Winter Olympics Opening Ceremony Disrupted by Malware Attack

The Pyeongchang Winter Olympics taking place in South Korea was disrupted over the weekend following a malware attack before and during the opening ceremony.

The cyber-attack coincided with 12 hours of downtime on the official website for the Winter Games, the collapse of Wi-Fi in the Pyeongchang Olympic stadium and the failure of televisions and internet at the main press center, leaving attendees unable to print their tickets for events or get venue information.

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.