WhatsApp users advised to update for protection

November 19 2019, by Nancy Cohen

Credit: CC0 Public Domain

A WhatsApp vulnerability could have put both iOS and Android users at risk. BGR.in referred to the flaw as "a specially-crafted malicious MP4 file."

The weakness could have allowed hackers to send a specially coded MP4 file. Reports said the vulnerability would allow hackers to trigger remote code execution (RCE) and denial of service (DoS) attacks.

The messaging app posted a security advisory about the bug, CVE-2019-11931, which affected earlier versions of the app on both Android and iOS devices. A stack-based buffer overflow could be triggered in WhatsApp.

TechRadar used its headline to tell readers: "Update WhatsApp now to protect yourself against a serious security risk."

WhatsApp fixed the vulnerability. Anthony Cuthbertson in The Independent on Monday said "A fix has been issued but users who have not downloaded the update for the latest version of WhatsApp are still vulnerable to the hack." As the flaw was fixed, that means newer software versions were now immune. Facebook told users to make sure they had the latest version of WhatsApp to be safe.

TechRadar similarly advised readers that "If you have a newer build of WhatsApp installed, you're safe—just run a check to see if there are any updates available for your handset."

Or, you could exercise the level of caution suggested by Chris Burns in SlashGear: "At this moment and for the foreseeable future, it's a good

idea to avoid opening MP4 files in WhatsApp. There's a bug in WhatsApp for both iOS and Android where a malicious person can send a specially-crafted MP4 file to ultimately control a users' phone. This bug was patched, but not all people in the world have said patch right this minute."

The same kind of advice could be found in *Digital Trends*. Be safe, not sorry. "Have you received a strange MP4 file on WhatsApp recently? It's probably best to avoid downloading it—at least until you update to the latest version."

(MP4, noted *Threatpost*, is a digital multimedia container format usually used to store video and audio, and attackers can exploit the flaw by sending a target user a specially crafted MP4 file,)

This was the advisory. "CVE-2019-11931 The vulnerability—tracked as CVE-2019-11931 —Description: A stack-based buffer overflow could be triggered in WhatsApp by sending a specially crafted MP4 file to a WhatsApp user. The issue was present in parsing the elementary stream metadata of an MP4 file and could result in a DoS or RCE. This affects Android versions prior to 2.19.274, iOS versions prior to 2.19.100, Enterprise Client versions prior to 2.25.3, Windows Phone versions before and including 2.18.368, Business for Android versions prior to 2.19.104, and Business for iOS versions prior to 2.19.100."

WhatsApp is a popular messaging platform. WhatsApp has over 1 billion users in over 180 countries. Earlier this month, *Digital Trends* said that "Since launching in 2009, WhatsApp has quickly become the world's most popular text and voice messaging application."

Reports said no users were impacted by the new vulnerability.