Issued 6/15/17

Windows Defender Antivirus Still Vulnerable to Attacks Despite Patches

Microsoft rolled out several patches for Windows Defender in order to address vulnerabilities that could have exposed Windows users, but it turns out that the company needs to do better because the antivirus is still suffering from a number of remote code execution flaws. A report from The Reg and citing security research James Lee reveals that the MsMpEng engine of Windows Defender is open to remote code execution due to insufficient sandboxing, a problem that some other security experts warned of in the last few months. Google's Tavis Ormandy, who previously discovered several major bugs in Microsoft software, also came across critical bugs in Windows Defender, and reported them to the company to have them fixed.

After patches for all these reported vulnerabilities were provided, Ormandy tweeted on June 7 to reveal that he found "more critical remote mpengine vulnerabilities," explaining that the antivirus engine needs to be sandboxed. The same problem is highlighted in today's report as well, as James Lee has discovered two remote code execution vulnerabilities that allow a system to get hacked despite running the very latest patches released by Microsoft. It appears that the new issues aren't related to the ones reported by Ormandy earlier this month and in late May, describing them as "multiple denial-of-service, integer overflow, and use-after-free bugs."