Trend Micro Hit By "Ridiculous" Flaw

Written by Marco Attard
14 January 2016

Security researchers at Google Project Zero warn of a dangerous flaw in the popular Trend Micro Antivirus security software opening a backdoor for PC hijacking, malware infection and password robbery.

According to the researchers, the flaw allows any website to run commands directly on PCs running Trend Micro software. Such commands including wiping the computer, downloading and installing malware and uninstalling Trend Micro antivirus. Posing the worst risk is the Password Manager component, since the application of a malicious script can steal all password stored on the browser, including encrypted ones.

"I don't even know what to say-- how could you enable this thing *by default* on all your customer machines without getting an audit from a competent security consultant?" researcher Tavis Ormandy writes in the Google Security Research blog. "You need to come up with a plan for fixing this right now. Frankly, it also looks like you're exposing all the stored passwords to the internet, but let's worry about that screw up after you get the remote code execution under control."

Ormandy is a veteran security researcher with experience exposing vulnerabilities in products from AVG, Kaspersky Lab, FireEye and Sophos.

In its turn, Trend Micro says the flaw was resolved once it Google revealed it (the research team gives companies 90 days to fix problems before making findings public) via security patch. But do ensure customers running Trend Micro Antivirus are updated to the latest versions.

Go TrendMicro node.js HTTP Server Listening on Localhost Can Execute Commands

Go Information on Reported Vulnerabilities in Trend Micro Password Manager