NETWORKWORLD

MICROSOFT EXPLORER
By Andy Patrizio

About |
Andy Patrizio is a freelance technology writer based in Orange County, California. He's written for a variety of publications, ranging from Tom's Guide to Wired to Dr. Dobbs Journal.

Password Manager flaw will hurt Trend Micro's reputation

The problem was addressed quickly but potential damage remains unknown.

Network World | Jan 15, 2016 6:51 AM PT

There is an inherent trust given to the makers of security tools, so when they screw up it really hurts. These are the companies we count on to keep us safe from malware. They are the last ones we want falling down on the job.

But unfortunately Trend Micro did just that and it was a doozy. A Google security engineer discovered a vulnerability in Trend Micro Password Manager, a part of the Trend Micro Antivirus product, and published it on a Google Security Research site on January 5. The bug would allow for the remote execution of code and possibly for passwords to be stolen.

The engineer, Travis Ormandy, noted "this product is primarily written in JavaScript with node.js, and opens multiple HTTP RPC ports for handling API requests. It took about 30 seconds to spot one that permits arbitrary command execution, openUrlInDefaultBrowser, which eventually maps to ShellExecute(). This means any website can launch arbitrary commands, like this:"

He then gave sample code showing how the Windows calculator could be launched, a benign activity. It could also do something far worse. One of the first responses he got was from someone at Trend Micro, and the conversation over the vulnerability played out in messages for everyone to read. Ormandy posted a sample string of code that could steal passwords from a password manager, even if they were encrypted, then use a remote execution to decrypt them.

"So this means, anyone on the internet can steal all of your passwords completely silently, as well as execute arbitrary code with zero user interaction. I really hope the gravity of this is clear to you, because I'm astonished about this," he wrote.

He also gave Trend a pretty hard time over the problem. "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?"

Six days later, Trend Micro pushed out a fix. In a post on the company's blog, Christopher Budd, who works in global threat communications, said Trend Micro's ActiveUpdates cannot be turned off, so all Trend Micro Password Manager customers have had the fix pushed out.

"For all intents and purposes, the reported critical vulnerabilities affect an old, no-longer available version of Trend Micro Password Manager," he wrote.

Perhaps, but it has undoubtedly left Trend Micro a little red-faced. Its antivirus is highly regarded and routinely scores at or near the top of antivirus tests. When you have that lofty a perch, much is expected of you, and the disappointment when you stumble is much greater.

So if you use Trend Micro Password Manager, you might want to consider changing your passwords, just to be safe.

Andy Patrizio

Andy Patrizio is a freelance journalist based in southern California who has covered the computer industry for 20 years and has built every x86 PC he's ever owned, laptops not included.

The opinions expressed in this blog are those of the author and do not necessarily represent those of ITworld, Network World, its parent, subsidiary or affiliated companies.

Must read: 11 hidden tips and tweaks for Windows 10

View Comments

Transfer Your Balance And Pay $0 In Interest For All Of 2016

LendingTree

Shark Tank Just Revealed a Trillion-Dollar Idea

The Motley Fool

Read Ebooks? Here's The Worst Kept Secret Among Book Lovers

BookBub

7 Credit Cards You Should Not Ignore If You Have Excellent Credit

NextAdvisor

2017 Chevy Bolt drive: This 200-mile EV could cure your range anxiety

7 wireless charging solutions

Nvidia's powerful Drive PX2 makes sense of the road

The Stunning Evolution of Millennials: They've Become the Ben Franklin Generation

The Huffington Post | Wealthfront