Written by Marco Attard
01 July 2016

Google researchers warn the core engine behind Symantec security products, including Endpoint Protection, features multiple critical vulnerabilities, putting "millions of computers" at risk.

"These vulnerabilities are as bad as it gets. They don’t require any user interaction, they affect the default configuration, and the software runs at the highest privilege levels possible," a Project Zero blog post reads. "In certain cases on Windows, vulnerable code is even loaded into the kernel, resulting in remote kernel memory corruption."

All Symantec and Norton branded antivirus products across all platforms pose the same security risks. Some of the flawed code is found in "unpackers," compression tools used to reduce executable sizes. Symantec runs unpackers in the kernel, leading to risks of clean heap overflow on Linux, Mac and other UNIX platforms, or kernel memory corruption in Windows.

The flaw is so bad victims simply need to receive a file-- no opening or futher interaction required-- to actually trigger it. As such, it is bad enough to allow an attacker to easily compromise an entire enterprise fleet.

Project Zero advises admins to take "immediate action" by proactively fixing all potential risk areas, since not all vulnerabilities can be repaired by automated updates. In turn Symantec has also released a series of security advisories.

Go How to Compromise the Enterprise Endpoint

Go Security Advisories Relating to Symantec Products