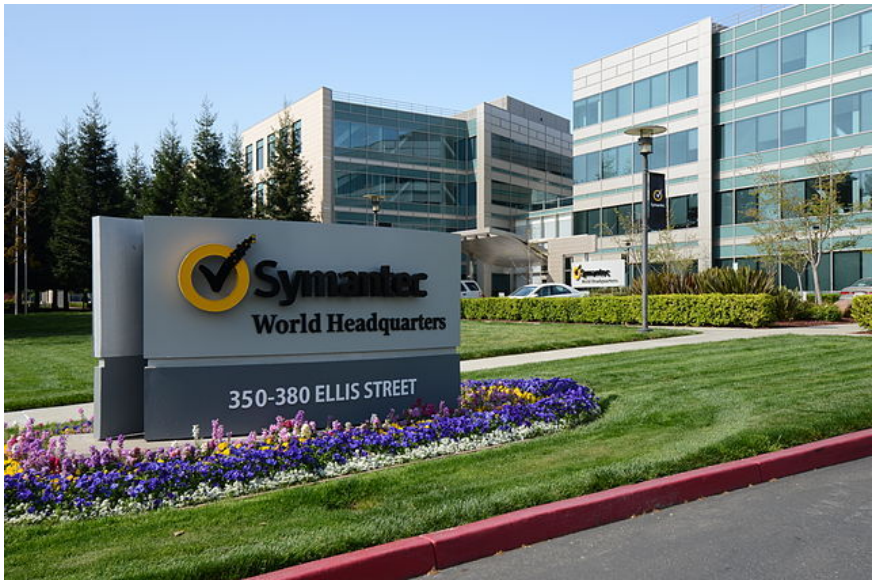
RISK ASSESSMENT / SECURITY & HACKTIVISM

High-severity bugs in 25 Symantec/Norton products imperil millions

If you use a Symantec or Norton product, now would be a good time to update.

by **Dan Goodin** - Jun 28, 2016 4:45pm PDT

87



LPS.1

Much of the product line from security firm Symantec contains a raft of vulnerabilities that expose millions of consumers, small businesses, and large organizations to self-replicating attacks that take complete control of their computers, a researcher warned Tuesday.

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

The post was published shortly after Symantec issued its own advisory, which listed 17 Symantec enterprise products and eight Norton consumer and small business products being affected. Ormandy warned that the vulnerability is unusually easy to exploit, allowing the exploits to spread virally from machine to machine over a targeted network, or potentially over the Internet at large. Ormandy continued:

> Because Symantec uses a filter driver to intercept all system I/O, just emailing a file to a victim or sending them a link to an exploit is enough to trigger it - the victim does not need to open the file or interact with it in anyway. Because no interaction is necessary to exploit it, this is a wormable vulnerability with potentially devastating consequences to Norton and Symantec customers.
>
> An attacker could easily compromise an entire enterprise fleet using a vulnerability like this. Network administrators should keep scenarios like this in mind when deciding to deploy Antivirus, it's a significant tradeoff in terms of increasing attack surface.

LATEST FEATURE STORY

FEATURE STORY (5 PAGES)

iOS 10 preview: Apple goes back to ignoring the iPad in a wide-ranging update

iOS 10 gives developers plenty to do and lets its users have a little fun, too.

WATCH ARS VIDEO

Ars delivers with Amazon Flex for a day

Sam becomes an Amazon Flex delivery man for a day.

STAY IN THE KNOW WITH

LATEST NEWS

Feds asked to investigate live-streamed death of motorist killed by cop

PASS CS:GO, COLLECT $200?

Mom takes on Valve, third-party "trading" sites, alleges "illegal scheme"

How an Illinois man's flag-burning 4th of July celebration ended in jail

CAVEAT EMPTOR

use to conceal their malicious payloads. The unpackers work by parsing code contained in files before they're allowed to be downloaded or executed. Because Symantec runs the unpackers directly in the operating system kernel, errors can allow attackers to gain complete control over the vulnerable machine. Ormandy said a better design would be for unpackers to run in a security "sandbox," which isolates untrusted code from sensitive parts of an operating system.

The researcher said one of the proof-of-concept exploits he devised works by exposing the unpacker to odd-sized records that cause inputs to be incorrectly rounded-up, resulting in a buffer overflow. A separate "decomposer library" included in the vulnerable software contained open-source code that in some cases hadn't been updated in at least seven years. The lack of updates came even though vulnerabilities had been found in some of the aging code and in some cases the disclosures were accompanied by publicly available exploits. A list of additional vulnerabilities is here.

Tuesday's advisory is only the latest to underscore game-over vulnerabilities found in widely available antivirus packages. Although the software is often considered a mandatory part of a good security regimen—on Windows systems, at least—their installation often has the paradoxical consequence of opening a computer to attacks that otherwise wouldn't be possible. Over the past five years, Ormandy in particular has exposed a disturbingly high number of such flaws in security software from companies including Comodo, Eset, Kaspersky, FireEye, McAfee, Trend Micro, and others.

In most cases, the updates disclosed Tuesday will be automatically installed, in much the way virus definitions are received. In other cases, end users or administrators will have to manually install the fixes. People running Symantec software should check the advisory to make sure they're covered.

READER COMMENTS 87

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.
@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE

Recode says

ON THE HOME STRAIGHT
Windows 10 Anniversary Update nears RTM with bugfixes galore

SAVE THE HABITAT
LucasArts' long lost, 30-year-old MMO is now preserved on Github

Contact Us
Reprints

SUBSCRIPTIONS
Subscribe to Ars

Visit Ars Technica UK

Vanity Fair
Style
Details

Visit our sister sites
Subscribe to a magazine

VIEW MOBILE SITE