CautelaLabs

Volume 2016-189-1

Symantec Security Flaw

Summary

Newly discovered vulnerabilities in Symantec's antivirus software include a flaw that could allow an attacker to remotely corrupt a computer's memory, security researchers announced this week. The vulnerabilities affect several Symantec products, including Norton antivirus software for consumers as well as enterprise solutions like Endpoint Protection and Mail Security for Microsoft Exchange. Symantec said it was not aware of the vulnerabilities being exploited, and has issued software updates that correct the flaws.

Detailed Information

"These vulnerabilities are as bad as it gets," they wrote. "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.

'Wormable' flaw that requires no user interaction by the victim

Unlike many computer viruses sent via email, which require the recipient to open an attachment in order to affect the system, the Symantec kernel vulnerability requires no user action.

That means that "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," the Project Zero team wrote. "Because no interaction is necessary to exploit it, this is a wormable vulnerability with potentially devastating consequences to Norton and Symantec customers."

Corrective Actions

The bugs have been patched, which is mostly good news since customers' software will be automatically updated. But some of the products "cannot be automatically updated," putting it on admins to "take immediate action to protect their networks."

Additional References

http://www.pcmag.com/news/345729/experts-symantec-security-flaw-is-as-bad-as-it-gets
http://www.computerworld.com/article/3089872/security/security-vulnerabilities-in-symantec-and-noton-as-bad-as-it-gets-warns-researcher.html