

Symantec patched vulnerabilities in antivirus software

Yesterday (May 30), software vendor Symantec patched the flaw in its corporate antivirus product line (English version), which was discovered nearly a week ago. The gap is on

Yesterday (May 30), software vendor Symantec patched the flaw in its corporate antivirus product line (English version), which was discovered nearly a week ago .

The flaw affects recent versions of Client Security and Antivirus Corporate Edition products. According to experts, the vulnerability is quite serious, can be exploited by hackers to run illegal software on the victim computer.



According to Symantec spokesman, the current patch is only for the English version of the above packages; Other full versions have not yet been announced.

Symantec did not reveal much information about the vulnerability, but according to eEye's warning, it was a kind of vulnerability that could be used to launch a form of self-attack - similar to the "Blaster" or Slammer "storm". in 2003.

However, according to Symantec, the company has yet to receive any notice of the status of the computer being attacked due to the vulnerability. The vulnerability only affects version 3.0 and later of Client Security; affect version 10 and later versions of Antivirus Corporate Edition. Norton antivirus products are not affected.

Reportedly, Symantec's security products have generated some pretty serious vulnerabilities. In December 2005, security researcher Alex Wheeler discovered a flaw in the Symantec (Antivirus Library) antivirus library, which could allow hackers to remotely attack and hijack a victim's computer running software. Symantec's -

(see at: <http://www.rem0te.com/public/images/symc2.pdf>). In October 2005, a serious vulnerability was discovered in Scan Engine software -

(see at: <http://www.symantec.com/avcenter/security/Content/2005.10.04.html>).

You finished reading the article "**Symantec patched vulnerabilities in antivirus software**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
