

Big Yellow Worm Alert! Protect Yourself!

Contributed by Wahoo Prime
Tuesday, 27 February 2007
Last Updated Monday, 05 March 2007

BIG YELLOW ALERT!

We've seen a lot of activity in the past day related to a problem with a vulnerability that attacks Symantec AntiVirus software. Yes we know that might seem like an oxymoron, but we didn't make it up either. We broke this two days before it became common knowledge. Read more about it here .

What software is affected? By the way, the worm is called "RINBOT", you can read more about it here . Unpatched Microsoft Windows PC's and user with Symantec Antivirus (versions below) are affected if they have not performed a recent update.

Symantec, Symantec Client Security, Version 3.1.400
Symantec, Symantec Client Security, Version 3.1.394
Symantec, Symantec Client Security, Version 3.0.2.2020
Symantec, Symantec Client Security, Version 3.0.2.2010
Symantec, Symantec Client Security, Version 3.0
Symantec, Symantec Client Security, Version 3.1
Symantec, Symantec AntiVirus, Version Corporate 10.1.400
Symantec, Symantec AntiVirus, Version Corporate 10.1.394
Symantec, Symantec AntiVirus, Version Corporate 10.0.2.2020
Symantec, Symantec AntiVirus, Version Corporate 10.0.2.2010
Symantec, Symantec AntiVirus, Version Corporate 10.0
Symantec, Symantec AntiVirus, Version Corporate 10.1

Some additional information indicates recent trends on this vulnerability appears to be related to an IRC BOT mostly aimed at colleges, but others, too. This link gives a rather good explanation of the exploit

<http://asert.arbornetworks.com/2006/11/that-new-bot-irc-bot-attacking-symantec-overflow/>

Helpful hints: Look in C:\Windows for w32svc.exe. That's a bad thing if you have it. Also, look in services for "Windows Network Firewall", another bad thing.

It might also be advisable to set your windows firewall to block ports TCP 445/2967/19555 & UDP 62050 in either direction until you are sure your software is properly updated.