McAfee joins Sophos, Avira, Avast—the latest Windows update breaks them all

Enlarge / A colorized transmission electron micrograph (TEM) of an Ebola virus virion. (Cynthia Goldsmith)

reader comments

162 with 110 posters participating

Share this story

The most recent Windows patch, released April 9, seems to have done *something* (still to be determined) that's causing problems with anti-malware software. Over the last few days, Microsoft has been adding more and more antivirus scanners to its list of known issues. As of publication time, client-side antivirus software from Sophos, Avira, ArcaBit, Avast, and most recently McAfee are all showing problems with the patch.

Affected machines seem to be fine until an attempt is made to log in, at which point the system grinds to a halt. It's not immediately clear if systems are freezing altogether or just going extraordinarily slowly. Some users have reported that they can log in, but the process takes ten or more hours. Logging in to Windows 7, 8.1, Server 2008 R2, Server 2012, and Server 2012 R2 are all affected.

Booting into safe mode is unaffected, and the current advice is to use this method to disable the antivirus applications and allow the machines to boot normally. Sophos additionally reports that adding the antivirus software's own directory to the list of excluded locations also serves as a fix, which is

a little strange.

Microsoft is currently blocking the update for Sophos, Avira, and ArcaBit users, with McAfee still under investigation. ArcaBit and Avast have published updates that address the problem. Avast recommends leaving systems at the login screen for about 15 minutes and then rebooting; the antivirus software should then update itself automatically in the background.

Avast and McAfee also provide a hint at the root cause: it appears that Microsoft has made a change to CSRSS ("client/server runtime subsystem"), a core component of Windows that coordinates and manages Win32 applications. This is reportedly making the antivirus software deadlock. The antivirus applications are trying to get access to some resource, but they're blocked from doing so because they have already taken exclusive access to the resource.

Given that patches have appeared from antivirus vendors rather than an update from Microsoft, it suggests (though does not guarantee) that whatever change Microsoft made to CSRSS is revealing latent bugs in the antivirus software. On the other hand, it's possible that CSRSS is now doing something that Microsoft previously promised wouldn't happen.

https://arstechnica.com/?p=1493563