

NT-Bugtraq: autorun problems after installing latest MS patches ms05-016 to -022 on Win2k server

autorun problems after installing latest MS patches ms05-016 to -022 on Win2k server

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-04/0041.html>

From: ntbugtrack (*ntbugtrack_at_APOLLOLIFESCIENCES.COM*)

Date: 04/13/05

Date: Wed, 13 Apr 2005 14:31:13 +1000

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Hi,

I was wondering if anyone else is experiencing the same problems or has some ideas what is going on.

After having installed manually the latest swag of MS patches ms05-016 to -022 on a Win2k server all seemed fine at first. I re-booted as necessary, all normal. I then logged in as an ordinary Domain user and was surprised that network drive mapping did not work nor had any of the autostart processes started – including the AVG antivirus on-access scanner. From a quick inspection with Sysinternals Autoruns (V6.0) I quickly determined that all entries in

`\Documents and Settings\ordinaryDomainUserMrX\Start Menu\Programs\Startup\`

`HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Run`
(and possibly others)

were not executed but the registry seemed intact. (Why the hack were they not executed – the registry entries all seem fine?). Not affected are software that run as services, such as a Kerio software firewall.

Strange thing – if I login as Domain Admin, the same processes that were not autostarted for the ordinary user, now all started as expected.... Logging off & logging in as Mr Ordinary again left the Antivirus and other autostarts dead again. Also I have ruled out the Kerio firewall as being a possible cause.

I have not tested this behaviour on a W2k workstation yet.

Anyone any good ideas?

Thanks,
Arndt

--

NT-Bugtraq: autorun problems after installing latest MS patches ms05-016 to -022 on Win2k server

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--