

APC Powerchute software – expired Java Runtime certificate has detrimental effect on Win2k / Win2k3 and SBS Servers

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-08/0012.html>

From: Michael Banjac (*michaelb_at_GENBM.COM.AU*)

Date: 08/12/05

Date: Fri, 12 Aug 2005 16:31:50 +0930
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

This week, we were baffled by a significant number of our managed client servers falling like dominos, each one exhibiting the same symptoms. Essentially, the consoles were dead or dead slow....couldn't open control panel or network properties, explorer was crashing (no desktop), IE was non responsive. Restart the server and the exact same symptoms reappear. Accessing the admin console across the network via RDP made no difference. At first sight, we were reasonably confident that the Server had been hijacked or hit by a virus.

Antivirus/antispam applications on each affected server were completely up to date and had detected nothing. We wasted hours scanning drives and searching for the problem through virus and adware forums. It was only by chance that one of our engineers noticed that there was a service that was still "starting". Once we eventually managed to change the service to manual startup and reboot the server, it was as happy as a lamb again.

Researching this further, we discovered that the services in question belonged to APC PowerChute Business Edition, in particular version 6.x. We now know that this version contains a Time Bomb (of sorts) that manages to cripple the server it's installed on. The problem is apparently related to a Sun Java Runtime Environment certificate contained within the software which was set to expire on the 27th July 2005. Even though this date had passed with no effect for many, once their servers were next restarted, the problem appeared. We could see that the processes themselves were loaded into memory but the services were still showing as "starting".

Once convinced that disabling the services would resolve the issue, we approached our remaining clients and performed the fix as a precautionary measure.

There is a posting on the APC site which describes this problem in some detail although they fall short of admitting that it affects servers as

T-Bugtraq: APC Powerchute software – expired Java Runtime certificate has detrimental effect on Win2k / Win2k3 and SB

badly as actually does. They mention that the software must be upgraded to version 7 to avoid future problems.

http://nam-en.apc.com/cgi-bin/nam_e...hp?p_faqid=7202
<http://nam-en.apc.com/cgi-bin/nam_e...hp?p_faqid=7202>

After the hours we wasted, I was livid that APC knew of this and didn't report it to their Distribution chain in the form of an alert so that it could be addressed prior to becoming a major issue. In the end, all that was required is a simple software upgrade to avoid this fracas.

Hopefully, this post will help some of you intercept and avoid this mind numbing, time wasting exercise.

Regards,

Mike Banjac
Genesis Business Machines
Adelaide, South Australia

--

NTBugtraq Editor's Note:

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

--