Article
Sean Connelly · May 15, 2017 2m read

Security Alerts

Wanna Cry

Most of you should be aware that the Wanna Cry virus is massively infecting un-patched windows machines all around the world. It's particularly affecting the NHS, one of my main clients.

Wanna Cry is one of a line of Viruses that exploit SMBv1 over ports 135 and 445.

A kill switch has been enabled, but this won't protect machines sitting behind http proxies, and there are already reports of new versions without a kill switch.

All windows machines should be isolated and updated a.s.a.p.

If automatic updates is not on, a patch can be dowloaded from here...

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Including the unusual security releases for XP and 2003...

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo...

To further protect these machines, enable port blocking on ports 135 and 445.

SMBv1 is a legacy service that is enabled by default, even on Windows 10 machines.

I have decided to completely disable this service on my internal machines without any issues, I found this command on stackoverflow...
dism /online /norestart /disable-feature /featurename:SMB1Protocol

Further considerations...

I run Malewarebytes (as well as Nod32) which reportedly can stop ransomware attacks before they can start encrypting files.

Obviously its also sensible to backup files just in case. Services such as drop box can restore previous versions of files that become encrypted. I also have a large external hard drive that stays disconnected. Every other week I connect it to do a backup.

I've also been thinking this morning about the locations some of my clients are backing up Cache dat files to. Many are just moving the dat files to a network drive. If a Caché machine becomes infected and encrypts the dat files, its highly likely that it could encrypt the visible network folder as well. Needs further consideration.

CIA Hacking Notepad++

I applied an update to Notepadd++ this morning and noticed this entry in the change log...

1. Fix CIA Hacking Notepad++ issue (https://wikileaks.org/ciav7p1/cms/page26968090.html).

I know of numerous clients / Caché developers that install Notepad++ on windows servers to read Caché log files etc. I'm not sure how the hack works but it would seem sensible for anyone using Notepad++ to update it a.s.a.p.

#Caché #Security

Source URL:https://community.intersystems.com/post/security-alerts