RM™
Education

Support
Newsletter

Issue 21

Included in this issue...
- Meltdown/Spectre vulnerabilities
- Support hot topics
- Recent, relevant articles
- BETT
- Upcoming seminars

Saji Mannalayil Markose
Technical Analyst, India

Support Newsletter

February 2018

Welcome to issue 21 of the support newsletter. This edition has our latest information and position on the Meltdown/ Spectre vulnerabilities, as well as including the normal security information, updates and development news. Please do feed back suggestions for content you'd like to see us cover – email us at **supportnewsletter@rm.com**. Please note you may be the only person within your establishment to receive this newsletter so please pass on to your colleagues.

An index of all released newsletters so far can be found in **DWN5175632**.

Network Security

We know how important securing your network is so we have highlighted a number of security issues that we believe are relevant to you and your networks.

Meltdown/Spectre vulnerability – latest news on the RM response to this
In early January reports started appearing about a new set of vulnerabilities that affect most of the computers in use today. We released a blog on this on 5 January with some background information. You can **read it here**.

We are also maintaining a couple of technical articles (open to all):
- Main article with our latest advice – available here in **TEC6034048**
- Article detailing available firmware updates for RM Recommends/RM Hardware – available here in **TEC6039891**

The current advice for customers is:

Meltdown

- This needs a patch for the operating system (OS).
- Before this patch can apply, you need a compatible anti-virus solution (as the AV needs to add a registry key to the client that then allows the OS patch to apply).
- RMVP customers need to either upgrade to RMVP 6.8 or move to Trend Micro (note that Trend Micro is our recommended solution for anti-virus). See **here** for more information.
- Please be aware that Microsoft is advising that the patches will incur some performance hit on the client.
- Currently the Microsoft patches (January 2018) need to be manually approved for your CC4 network (as there is an issue that can break RMVP 6.6 or earlier) – thus once you have a compatible anti-virus solution, you will need to manually approve the patches (**see here**).
- Windows servers need additional registry keys to activate the patch on the server – CC4 customers can do this via CC4UPD211 (we will also publish batch files for vanilla servers on our main article - **TEC6034048**).

Spectre

- This has two variants – the first can be patched via updated firmware from the hardware vendor – customers with RM computers should monitor **TEC6039891**.
- The second is a software-based issue and we are reviewing the advice from Microsoft and vendors relating to this.

WSUS approvals 22 February

- We will be switching back to automatic approvals of Microsoft patches from 22 February (so that you continue to be protected).
- As Microsoft patches (for Windows 10 and Server 2016) are cumulative, then the Meltdown patches will start to apply then.
- CC4 RMVP (SEP) customers thus need to ensure that by this date they have either:
  a. Upgraded to Trend Micro (our recommended option).
  b. Upgraded to RMVP 6.8.
  c. Disabled automatic approvals in the RMMC (see **TEC6058976**) – although you should view this as a "last resort" action if you cannot complete (a) or (b) in the timescales.

Support hot topics/CC4 updates

Recent CC4 updates can be found in the article **TEC1255704** as usual (note that we have recently reduced the size of this article and put the archived updates in '**TEC5733502** - Archive of Community Connect 4 (CC4) software updates'). CC4 updates in development can also be reviewed in **TEC2625548**.

Some recent CC4 updates include:

CC4 update/ DWN	Description	More information
CC4UPD210 **DWN6010523**	A new version of the package (RM Update Build Certificate) that was delivered originally by CC4UPD203.	Recommended if you are using LST (Local Support Tools) to rebuild computers manually. The package adds the new CC4 Build Certificate to the recovery partition on your computers (so that remote rebuilds can work) and fixes an issue where the X: drive may have remained mapped to this partition.
CC4DRV113 **DWN5587087**	Driver Update 113 for Community Connect 4 networks [CC4DRV113]	Re-issued having been reworked to address a security issue with the included Synaptics Touchpad driver.
CC4DRV111 **DWN5549892**	Driver Update 111 for Community Connect 4 networks [CC4DRV111]	Re-issued having been reworked to address a security issue with the included Synaptics Touchpad driver.

Note on terminology used in the article:

CC4.3 – your CC4 First server is running Windows 2008R2 server
CC4.5 – your CC4 First server is running Windows 2012R2 server
CoP – Connect on Prem - your CC4 First server is running Windows 2016 server

Some recent, relevant articles

Articles

Article reference	Description	More information
TEC6034048	Meltdown/Spectre vulnerability	Our main article on the Meltdown/Spectre vulnerability. See above security section.
TEC6039891	RM Recommends/hardware client and server firmware updates following the Meltdown/Spectre vulnerability	We are keeping this article up to date with firmware (BIOS/UEFI) updates from our vendors.
TEC6045007	How to apply the January 2018 Meltdown Windows updates via WSUS	As above – all CC4 customers will need to manually approve the January 2018 Microsoft patches. RMVP customers need to be on RMVP 6.8 (or move to Trend) before approving the patches.
TEC6041686	Trend Micro on-premise and the Meltdown vulnerability	Provides details on upgrading the on-premise version of Trend so that your clients are ready for the Meltdown patch.
TEC6066087	How to find out which version of RM Virus Protect (RMVP) is installed	
TEC6058976	How to turn off the automatic approval of updates within RM WSUS	This is not a recommended approach from RM – but provided for those customers who cannot move to a compatible anti-virus by the 22nd February (see above).
TEC6046757	Protecting Chromebooks from Spectre/ Meltdown vulnerabilities	Provides steps to protect Chromebooks from Spectre/Meltdown vulnerabilities.
TEC6002776	RM Cloud Backup - D2D2C recovery point creation failure	Describes an issue that may affect Cloud Backup customers using Trend Micro.
TEC6018218	Common Community Connect 4 (CC4) user management issues	An index article to a number of common, RMMC user manager issues.
TEC6018411	CC4 RMMC may show an "out of memory" error during User Management tasks	Details a known issue where customers experience memory errors during CC4 user management tasks. We have found that upping the memory to 16GB helps.
TEC5573761	How to update the MARS Agent for RM Cloud Backup	
TEC6013709	DefaultUser0 account on Windows 10 version 1607 computers	
TEC6007570	Potential security risk if you have the X: drive assigned to CC4 computers	Details the issue addressed by CC4UPD210.
TEC6035776	Overrunning scheduled scans in Trend Micro	
TEC5771690	How to enable data encryption within Veritas Backup Exec 16	
TEC6043995	Patch a standalone ESXi host or ESXi hosts in a Cluster without using vCenter Update Manager	
TEC6035512	HP notebook computer battery safety recall and replacement program (2018)	

Also, do visit the **CC4 portal** on the RM Support website for the latest editor's choice and technical articles.
For the full list of CC4 Assured hardware please see **TEC1299560**.

Recent updates

CC4 roadmap
We have recently published the CC4 Roadmap in a public facing Trello board - **trello.com/b/wIPMZM7X/rm-cc4**. Here you will find information on the roadmap, what's up next in development, in trial, etc. – with a chance to vote (or submit suggestions) for CC4 roadmap items.

RM Unify Network Provisioning and password policy
Customers taking the RM Unify Network Provisioning add-on will now be subject to the RM Unify password policy when changing passwords (see **TEC5943089** for more information).

Note that RM Unify checks passwords in a different way to the traditional Active Directory – thus if you are using this feature, then we recommend that you change passwords within RM Unify and let these cascade down to your network.

Windows 10 v1709 (Creators Edition Fall Update)
We are currently working on the next version of Windows 10 for CC4 (v1709 – the Creators Edition Fall Update) and hope to have this available in early spring 2018. We will release this as both a new WIM file (for fresh builds) and also as a WSUS option for in-place upgrades (note that due to limitations in Windows Server 2008R2 and WSUS, CC4 customers with this as their CC4 First server will not be able to deploy the in-place upgrade option).

RM Supported Technologies List
The latest version of this list, including support for Server 2016, MABS, Trend Micro, etc. can be found here: **Supported Technologies**

Other news...

Did you see us at BETT?
We were back at BETT this January and had lots of great conversations with you on the stand as well as listening to a lot of the speakers around the show. If you didn't get to chat to us at BETT, you can see what we were talking about on the stand at **rm.com/bett18**.

Join us on our upcoming webinars
Take a look at the list of upcoming webinars on **rm.com/events/webinars** and sign up for free today. In February, Steve Forbes, our Senior Product Manager for safety and security, will be running two 'Security & compliance' webinars - well worth a watch if you want to understand the insider threat to schools and the security options available to you.

RM Spring Seminars 2018
The first dates and venues have now been announced for the upcoming RM Seminars.
•   Birmingham – 5th March
•   Stansted – 7th March
•   Cardiff – 9th March
•   Exeter – 12th March
•   Warrington – 21st March

Expect more dates to follow! You can sign up today at **rm.com/seminars**.

Meet the team

Saji Mannalayil Markose
Technical Analyst

Saji is a Technical Analyst in the Networks Support team. He has been working with RM since 2010 after graduating with a B-Tech in Electronics and Communication, from Mahatma Gandhi University.

He started with supporting CC4, and now works in Wireless and Apple support too as well as helping with the installation Service Desk during busy periods. Saji has received a number of customer experience awards and nominations. Saji is fond of music when outside work, and used to play the piano and compose jingles. He also loves travelling, playing cricket (as an all-rounder) and watching movies (a particular favourite is The Dark Knight Rises).

Look out for the next issue!

Email any suggestions to
supportnewsletter@rm.com