RM ™
Education

Support
Newsletter

Issue 22

Included in this issue...

- Security – our latest on Meldown/Spectre
- Windows 10 v1709 (Creators Edition Fall Update)
- TLS 1.0 removal from RM.com websites and how it affects you
- Office 365 Security Services
- RM Services for Intune for Education

Damian Rusling
Support Consultant

Support Newsletter

March 2018

Welcome to issue 22 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
We have released CC4UPD211 and also now switched back to business as usual in terms of approving WSUS updates for CC4 – so the February releases should have started to apply on to your network. The anti-virus guidance given **here** still applies to RMVP customers as the updates are cumulative.

Support hot topics/CC4 updates

Recent CC4 updates can be found in the article **TEC1255704** as usual (note that we have 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 updates include:

Update/DWN	Description	More information
CC4UPD211 **DWN6046461**	Provides the necessary registry keys so that the Microsoft Meltdown patch becomes enabled on the CC4 server	Recommended for all customers as this protects against the Meltdown vulnerability. Please see the article for feedback from our performance testing of CC4 servers.
CC4DRV119 **DWN6118420**	Driver Update 119 for Community Connect 4 networks [CC4DRV119]	Download to install updated drivers for use during computer builds on Community Connect 4 (CC4) networks.
DWN6050841	GPO to enable Windows Remote Management	Provides the GPO to enable Windows Remote Management (WinRM).
DWN6094620	RM Virus Protect 6.8 Release Note for CC4	Instructions for installing, using and uninstalling RMVP 6.8.

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	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.
TEC6047337	How to renew your CC4 Anywhere NetScaler 10.5 certificate	Contains the steps to renew your CC4 Anywhere NetScaler 10.5 certificate.
TEC6086591	How to transfer a user from one RM Unify establishment to another	Describes the options for user account transfers between RM Unify establishments.
TEC5823985	Authoritative restore of Active Directory objects	How to restore objects which have been deleted from Active Directory.
TEC6090000	Speculation Control Validation PowerShell Script for Meltdown and Spectre vulnerabilities	PowerShell script to remotely query Windows computers to determine if protected against Speculation Control Exploit (Meltdown\Spectre).
TEC6094744	RM Virus Protect 6.8 for Community Connect 4	If you have a current RMVP contract, you are entitled to this update. It will be in your My Account area.
TEC6097463	How to configure Information Rights Management (IRM) for Microsoft OneDrive and SharePoint Online document libraries	Steps on how to configure IRM for Microsoft OneDrive and SharePoint Online document libraries.
TEC6097467	Install the Azure Information Protection client for users	The procedure in this article is relevant if you have purchased or implemented the Office 365 Data Protection Service from us.
TEC6103448	Microsoft .NET Framework 4.6.2 for Community Connect 4 networks	Download and instructions for installing Microsoft .NET Framework 4.6.2 for Community Connect 4 networks.
TEC6099702	Expected behaviour of Office desktop apps with an RM Unify federated Office 365 account	Explains the expected behaviour when accessing locally installed Office desktop apps when you have an Office 365 domain federated to RM Unify.
TEC6041874	Unable to build computers with the default assignments after CC4.3 to CC4.5 upgrade	Explains why you are unable to build computers with the default assignments after a CC4.3 to CC4.5 upgrade and contains a workaround.
TEC6052899	How to remotely query Windows update history on a computer	Instructions and Windows PowerShell script providing details on how to remotely query Windows update history.

TEC6057740	Error "This field cannot be empty" displayed when modifying RM Tutor 6.1 registry policies	How to resolve an issue when configuring Broadcast Address registry policies for RM Tutor 6.1.
TEC6066087	How to find out which version of RM Virus Protect (RMVP) is installed	Includes the RMVP versions we've released along with the corresponding SEP (Symantec Endpoint Protection) version.
TEC6072091	When signing out of RM Unify, you are unsure if your G Suite or Office 365 session has been signed out	Explains why users may not see a green tick next to G Suite or Office 365 when signing out of RM Unify.
TEC6137461	CC4 Access technical overview	An overview of the main elements of CC4 Access.
TEC6123297	Critical alert "Volume missing" displayed in RM Cloud Backup - D2D2C	Covers why the critical alert "Volume missing" is displayed in RM Cloud Backup - D2D2C.

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/wlPMZM7X/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.

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). The
first phase of this has now been released and this delivers a new WIM (build image) for you to rebuild computers
fresh to this new version of W10. This is available in your My Account area on RM.com if you are eligible. The WSUS
in-place upgrade will follow a little later as we are just finalising the field trials of this.

Note: 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 Services for Intune for Education now available
The much anticipated Intune for Education RM services are now available. Whether you have existing or new
devices, shared or 1-1, we have a service to get you set up for supporting those devices with Intune for Education;
the cloud based device management software designed for education.

Contact your account manager or email our sales team at **networks@rm.com** to discuss your requirements, and
understand how Intune for Education can help you provide a highly flexible and modern way of managing your
Windows 10 devices.

RM Unify v3.36 released

Linked somewhat to the Intune for Education project, v3.36 includes a fix to allow RM Unify provisioned Azure AD users to log into Azure AD joined (Intune managed) devices. This means you can now use RM Unify to provision and manage users for both Intune for Education managed devices and CC4 managed devices.

TLS 1.0 removal from RM.com websites

Transport Layer Security (TLS) is a cryptography protocol that is used for the majority of secure HTTPS websites. There are multiple versions of TLS; the most current release is TLS v1.2. TLS v1.2 is widely supported by all current Internet browser software.

An industry wide program has been initiated by the **PCI Security Standards Council** to ensure that TLS v1.0 is disabled for all websites that accept secure payments by 30 June 2018.

What are we planning to do?

In May 2018 (*), we will disable TLS 1.0 support for the following websites:

- shop.rm.com – RM Store
- rmbookspayment.rm.com – RM Books payment service
- esi.swgfl.org.uk – SWGfL Electronic Service Interface
- support.rm.com – RM Support Online
- account.rm.com – RM My Account
- partners.rm.com – RM Partner Programme Portal

(*) exact date still to be confirmed.

What do you need to do?

If your network uses modern Internet browser software then it is likely that no action is required. Specifically, TLS v1.2 is enabled by default on the following versions:

- Microsoft Edge
- Internet Explorer 11
- Google Chrome v33 or above
- Firefox v27 or above
- Safari v7 or above (Mac OS X v10.9+)

If your network uses Windows 7 with Internet Explorer 10 or below, then there are a set of steps that will be required to enable TLS 1.2 support. **Please refer to RM Support Online where we will keep you up to date on the latest information on this change.**

If your network uses older operating system software then you may find you are not able to access these websites, and a wide range of other public websites that take secure payments, from 30 June 2018.

Office 365 security services

Microsoft Office 365 is a secure platform that is available for free for UK educational establishments. Whilst it is easy to set up and get going on the platform – it is a little harder to ensure that all the correct settings and alerts are established to ensure you have the security at a level that you are comfortable with.

Microsoft offer a free tool called Secure Score that tells you how secure your environment is and makes some recommendations as to how you might improve that score. We offer a range of services that can help you secure your Office 365 platform, as well as protect your user identities and their data from potential threats:

Office 365 message encryption – £155

We will configure Office 365 message encryption for you to ensure your data is secure when being emailed to an external person, school or company.

Azure AD Identity Protection Service – £465

We will add an additional layer of security to your Office 365 credentials, configuring policies that give you full control over the acceptable risk levels in your school and enforcing things like multi-factor authentication should the risk be too great.

Office 365 Advanced Threat Protection – £465

Office 365 Advanced Threat Protection protects your email, OneDrive, SharePoint and Teams from malicious attachments and URLs, malware and phishing attempts.

Office 365 Data Protection Service – £610

We will configure Azure Information Protection and Data Loss Protection policies for your Office 365 environment, to ensure that your users can label their documents with a sensitivity rating and apply policies to restrict the movement of that data.

We can also provide an auditing service that checks your Office 365 secure score and we will make agreed changes to increase your overall score - £610.

For further details, please email **networks@rm.com** or contact your sales account manager. Please note additional licences may be required for some features.

Other news...

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

Join us on our upcoming webinars
We have just updated our webinar calendar to provide you with a series of webinars covering a variety of topics – from safeguarding and GDPR compliance, to roadmap updates and everything in between. Sign up for free to any of our upcoming webinars at **rm.com/webinars**.

RM Community

We've just added two new groups to the RM Community for the topical subjects of data protection and online safety. As well as giving you a specific area to share knowledge, we will also use these forums to discuss how you can make sure your data and users are protected.

For those of you that have registered but don't use the community, you may now want to get involved as this is where our product managers and developers share information and respond to your questions. It is easy to access using the link **community.rm.com/community.** You just need to sign in with your RM Unify username and password. If you haven't yet registered then please see **NWS4094307**.

Data protection
Data protection, GDPR

Online safety
Keeping your users safe online

Meet the team

Damian Rusling
Support Consultant

Damian is a support consultant in the Networks and Enterprise Support team.

He joined RM as a fresh faced 20 something in 1999. Prior to that Damian gained a BA (Hons) in Sociology and Politics, followed by a Postgraduate Diploma in IT and then undertook a couple of IT support jobs in and around Glasgow.

As a long-term member of the team, Damian has supported Community Connect in all its variations from CC2.3 onwards. Current supported technologies include CC4, Vanilla Windows and VMware. Damian is lucky enough to have spent some time in the RM Indian office including a four month secondment. This gave him the opportunity to explore the beautiful state of Kerala and enjoy the local culture and cuisine.

Outside of work Damian is an avid football fan and goes to every Celtic home game. He also enjoys trying to keep fit via cycling and walking. Live music and comedy is also high on Damian's list of activities and he has seen his favourite bands, the Manic Street Preachers and Teenage Fanclub, too many times to count. He has also been known to attend the occasional musical theatre event with his wife.

Look out for the next issue!

Email any suggestions to
supportnewsletter@rm.com