

First Release: 19 May 2017

Subject: WannaCry Ransomware and SMB V1.0 exploit



Announcements contain information that may be superseded. Please contact NTS if you are not sure whether the information is relevant to your particular situation.

Details:

Issue :

WannaCry ransomware is spreading worldwide and many computers have been infected by it. Systems successfully infected with WannaCry will scan random IP addresses very rapidly (about 25 IP addresses per second) for open TCP 445 ports (the port used for SMB communications) and if open will attempt to spread the WannaCry infection using the EternalBlue SMB exploit.

This malware targets computers running Windows OS, so our MFP and Laser Printer products cannot be infected.

Resolution :

Microsoft has announced the following guidance in response to this attack.

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

In this announcement, it is suggested that the security patch (MS17-010) <https://technet.microsoft.com/en-us/library/security/ms17-010.aspx> be applied.

In addition to applying the security patch, Microsoft advises that SMB v1.0 should be disabled on computers as a workaround.

Based on Microsoft's advice, it's expected that some customers will disable SMB v1.0 and/or ask Ricoh about the effects of disabling SMB v1.0. If SMB v1.0 is disabled then several functions will no longer work, so related inquiries may increase at call centres and help desks.

When SMBv1.0 is disabled the following functions will be unavailable because our MFPs only support SMB v1.0.

- Scan to Folder
- Fax Transmission backup to Folder (SMB only)
- Fax Forwarding (SMB only)

We are now checking whether other functions are affected.

The following products support SMB v2.0 and are therefore not affected:

SP C220S / C222SF.
SP C231SF / C232SF
SP C240SF / C242SF
SP C250SF / C252SF
SP 3400SF / 3410SF
SP 3000SF / 3510SF

Workaround

If SMB v1.0 is disabled, the following can be used as alternatives to Scan to Folder.

- Scan to E-mail
- Store the file to a Document Server and then retrieve it via Web Image Monitor
- Scan to URL
- Scan to Media

Plan

Ricoh has a plan to support SMB v2.0 / v3.0. We will inform you of the schedule as soon as it is decided.

Documents:

N/A