3xLOGIC

Service Bulletin 170023

3xLOGIC – Assessment and Response – WannaCry Ransomware Worm

Service Bulletin #:	170023-2
Date:	May 13th, 2017
Product Affected:	3xLOGIC DVR/NVR/VMS systems running supported versions of Microsoft Windows OS
Purpose:	This document is intended to provide readers with 3xLOGIC's assessment and response to the recent EternalBlue / WannaCry Ransomware Worm attacks.
***Importance:**	High

1 Assessment

On May 12th, 2017, reports of the *WannaCry* (*WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY*) *Ransomware Worm* attacking business systems began to surface across the globe. The *WannaCry* virus exploits vulnerabilities in the Windows SMB Server to potentially take control of a system's contents and demand a ransom from the system operators to release the system's contents back to the owner.

The infection vector of the WannaCry attacks has been recognized as the *EternalBlue* exploit. All Windows systems actively supported by Microsoft (as well as Windows XP) are affected.

On March 14th, 2017, Microsoft released a windows security update to safeguard systems from *EternalBlue.*

- *Security Update for Microsoft Windows SMB Server (4013389).*

On May 15th, 2017, after the onset of attacks, Microsoft also released an update for the unsupported Windows XP OS:

- *Security Update for Windows XP SP3 (KB4012598)*:

As a response to the recent attacks, 3xLOGIC has also issued a patch in the form of a VGL update package:

- *DisableSMBV1.vgl*

For information and instructions on applying these updates to safeguard your VIGIL system(s), navigate through the remainder of this bulletin.

2 Response

As all 3xLOGIC VIGIL NVR/DVR/VMS systems run on various versions of the Windows operating system, these systems, if not updated, are potentially at risk.

2.1.1 3xLOGIC VIGIL VGL Package

As an immediate response, 3xLOGIC has engineered an update package which can be applied to a system to disable SMB1. This vgl package works for both Windows 7 and Windows XP systems. It can be pushed via VIGIL Central Management (VCM) for mass deployment or by manually transferring the package and running it on the system in question. This will remove the immediate risk associated with Eternal Blue / WannaCry.

To acquire the 3xLOGIC VGL File, visit the below link:

- **3xLOGIC VGL Disable SMB1 Patch** - http://www.3xlogic.com/software/disablesmbv1zip

Once you have applied the .vgl package, the system is no longer "at risk". However, 3xLOGIC highly recommends also applying the appropriate Microsoft Security Update as an added security measure. Navigate to the next section of this bulletin for more information.

2.1.2 Microsoft Security Update 4013389 / KB4012598 (WinXP)

After applying the .VGL package, 3xLOGIC also highly recommends all VIGIL system administrators check to confirm the official Windows update for their Windows version; *Security Update for Microsoft Windows SMB Server [4013389]* or *Security Update for Windows XP SP3 (KB4012598),* has been applied to their 3xLOGIC NVR/DVR/VMS systems. If this update has not been applied, 3xLOGIC requests administrators download and apply the SMB Server security update to safeguard their system against possible infection.

To acquire and apply the Windows SMB Server security updates, visit the appropriate link below link:

- **Microsoft Update (Windows XP Only)** - https://www.microsoft.com/en-us/download/details.aspx?id=55245
- **Microsoft Update (All Other Windows Versions)** - https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Once the *.vgl* package and appropriate Windows update have been applied, your system should be considered secure against infection by *EternalBlue* / the *WannaCry Ransomware Worm*.

3 Contact Information

If you require more information, or if you have any questions or concerns, please contact 3xLOGIC Support:
Email: helpdesk@3xlogic.com
Online: www.3xlogic.com

*** Importance:**	High	Mandatory Upgrade – Will affect the recording functionality of the VIGIL Server System and may cause loss of video records
	Medium	Recommended Upgrade – Will not cause loss of video records, may affect usability of the System.
	Low	VIGIL Server System will function properly – Affects non-critical system features only.