Service Bulletin 180003

3xLOGIC - Intel® Spectre and Meltdown Vulnerability - Assessment and Response

Service Bulletin #:	180003-3
Date:	January 18th, 2018
Revised:	March 2nd, 2018
Product Affected:	VIGIL VMS / DVR Systems running Windows 7 Embedded SP1
Purpose:	This document is intended to provide the reader with 3xLOGIC's assessment and response to the recently identified Intel® Spectre and Meltdown vulnerabilities.
***Importance:**	High

1 Assessment

On Jan. 3, 2018, security researchers publicly detailed three newly discovered potential vulnerabilities in Intel based systems named Meltdown and Spectre (Variant 1 and Variant 2).

Information regarding these vulnerabilities has been disseminated by several online blogs and forums and is widely available. For more information, a detailed technical analysis can be found via Stratechery. A shorter summary of these vulnerabilities is provided on the Microsoft Cloudblogs here, with an excerpt regarding potential impact below:

> On Intel-based phones or PCs, malicious software could potentiality exploit this silicon vulnerability to access information in one software program from another. These attacks extend into browsers where malicious JavaScript deployed through a web page or advertisement could access information (such as a legal document or financial information) across the system in another running software program or browser tab. In an environment where multiple servers are sharing capabilities (such as exists in some cloud services configurations), these vulnerabilities could mean it is possible for someone to access information in one virtual machine from another.

For more details , please visit the below links:

- https://stratechery.com/2018/meltdown-spectre-and-the-state-of-technology/
- https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/
- https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)

2 Response

To mitigate these vulnerabilities on 3xLOGIC VIGIL VMS / DVR systems , 3xLOGIC Engineering has constructed a VGL patch (*VIGILServerUpdate(WES7_Intel_Kernel_Memory_Leak v9_99_9999.vgl)* for VIGIL systems running Windows 7 Embedded SP1. Details regarding each vulnerability are available in the below table:

Exploited Vulnerability	CVE	Exploit Name	Public Vulnerability Name	Windows Changes	Fix included in VGL
Spectre	2017-5753	Variant 1	Bounds Check Bypass	Compiler change; recompiled binaries now part of Windows Updates Edge and IE11 hardened to prevent exploit from JavaScript	YES
Spectre	2017-5715	Variant 2	Branch Target Injection	Calling new CPU instructions to eliminate branch speculation in risky situations	NO (Intel firmware update required. Awaiting firmware from Intel).
Meltdown	2017-5754	Variant 3	Rogue Data Cache Load	Isolate kernel and user mode page tables	YES

2.1 VGL Components

The following components are installed using the VGL:

- https://support.microsoft.com/en-us/help/4056897/windows-7-update-kb4056897
- http://www.catalog.update.microsoft.com/Search.aspx?q=KB4056897

2.2 Downloading and Installing the VGL

To safeguard your system by installing the patch, follow the below instructions:
Download the VGL patch here (or request a copy from a 3xLOGIC Support Representative). Once downloaded, launch the file and follow the on-screen instructions to complete the installation.

Notes:

If you want to push the VGL through VCM, you will need to upgrade your VCM to 10.00.0200 or later to use this VGL.

If you want to run the VGL locally in DVRs with v9.5 or older software, please update the VIGIL local updater first. Download the latest version here or request it from a 3xLOGIC support representative.

Once installed, your system will be secure against the vulnerabilities as listed in the table in Section 2.

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.