Datalogic Security Bulletin

Last Update: April 27, 2018

SPECTRE AND MELTDOWN ISSUE

Spectre and Meltdown are security vulnerabilities that affect many modern processors. They are "speculative execution side-channel attacks" that can lead to un-wanted information disclosure. They manifest themselves in 3 variants:

- CVE-2017-5753 - Bounds check bypass (Spectre)
- CVE-2017-5715 - Branch target injection (Spectre)
- CVE-2017-5754 - Rogue data cache load (Meltdown)

Datalogic is actively pushing its operating system and chipset vendors for a formal risk assessment and timeline for patch if required. Meanwhile, there have been no reports of exploits involving Datalogic devices.

Datalogic devices are not general-purpose consumer products. Rather, they are purpose-built for use in a business environment. As such, they typically operate in controlled environments with limitations on access, usage, and loading of software. This greatly reduces the likelihood of malware attacks on Datalogic products.

Datalogic applies security best practices throughout its processes. Many Datalogic devices include lockdown utilities, which helps keep systems safe and secure. Datalogic also monitors security bulletins for CVEs and provides firmware patches accordingly.

WHAT DO WE RECOMMEND

With that being said, cyber security is multi-layered and cross-functional, and requires commitment and teamwork. Effective security is accomplished through the integration of multiple efforts and the sharing of knowledge and intelligence between vendors, customers, and all community members. Datalogic strongly encourages customers to undertake safe security measures, including:

- **Use strong password protocols:** The use of strong passwords can slow or often defeat the various attack methods of compromising a device's security.

- **Use secure networks:** When you connect through an unsecure network, anyone in the vicinity can monitor the information passing between your device and the WiFi router if your connection is not encrypted. If you use a service that encrypts your connection to the web service, it can make it much more difficult for someone to snoop on your activity.
- **Adopt regular software updates:** Update your operating system, web browser, and CPU firmware as those become available
- **Avoid unknown sources:** Only download software and apps from reputable or approved sources to reduce the risk of malware infection.
- **Antivirus/security software:** This helps prevent hackers from gaining access to your devices in order to install the malicious software to exploit various vulnerabilities.
- **Lockdown devices:** Datalogic and various 3rd parties offer utilities to lockdown your device/computer to prevent un-authorized access and to limit outside exposure or even which applications can run on the device.

STATUS OF DATALOGIC PRODUCTS

Mobile Computers			
Product	**OS**	**Processor**	**Status**
Joya Touch			
	Android 6, Android 7	Qualcomm SnapDragon 8909	Not impacted
	WEC7	Marvell XScale™ PXA310	Not impacted
X3 products			
Lynx	WEHH 6.5	Marvell XScale™ PXA310	Not impacted
Memor X3	Windows CE 6.0	Marvell XScale™ PXA310	Not impacted
Skorpio X3	WEHH 6.5, Windows CE 6.0	Marvell XScale™ PXA310	Not impacted
Falcon X3+	WEHH 6.5, Windows CE 6.0	Marvell XScale™ PXA310	Not impacted
X4 products			
Skorpio X4	Android 4.4, WEC7	TI OMAP 4430	Not impacted by Meltdown. Spectre under investigation.
Falcon X4	Android 4.4, WEC7	TI OMAP 4430	
DL-Axist			
	Android 4.4	TI OMAP 4430	Not impacted by Meltdown. Spectre under investigation.

Soredi

Product	Processor	OS	Status
SH10, SH12			
	ARM QMX 6 Quad, 4 x 1.0 GHz, 1GB	WEC7	Under investigation
	Intel® E3826, 2 x 1,46 GHz Dual-Core, 4 GB RAM	Win 7 Pro, Win 7 Emb, WEC7, Win10 Pro, Win10 IoT	Under investigation
	Intel® E3845, 4 x 1,91 GHz Quad-Core, 4 GB RAM	Win 7 Pro, Win 7 Emb, WEC7, Win10 Pro, Win10 IoT	Under investigation
	Intel® Core i3-5010U, 2 x 2,1 GHz, 4 / 8/16 GB RAM	Win 7 Pro, Win 7 Emb, WEC7, Win10 Pro, Win10 IoT	Under investigation
	Intel® Core i5-5350U, 2 x 1,8 GHz, 4 or 8 GB RAM	Win 7 Pro, Win 7 Emb, WEC7, Win10 Pro, Win10 IoT	Under investigation
Rhino II			
	ARM QMX 6 Quad, 4 x 1.0 GHz, 1GB	WEC7, Android 7	Under investigation
	Intel® E3826, 2 x 1,46 GHz Dual-Core, 4 GB RAM	Win 7 Emb, Win10 IoT	Under investigation
TaskBook v1			
	ARM QMX 6 Quad, 4 x 1.0 GHz, 1GB	WEC7	Under investigation
	Intel® E3826, 2 x 1,46 GHz Dual-Core, 4 GB RAM	Win 7 Emb, Win10 IoT	Under investigation
SH15, SH21			
	Intel® E3845, 4 x 1,91 GHz Quad-Core, 4 GB RAM	Win 7 Emb, Win10 IoT	Under investigation
	Intel® Core i5-5350U, 2 x 1,8 GHz, 4/8/16 GB RAM	Win 7 Emb, Win10 IoT	Under investigation

Vision Systems

Product	Processor	OS	Status
MX-E80 MX-U81 MX-U80	Intel Core i7 3615QE 2.3 Ghz – quad core	Windows Embedded Standard 7 32 and 64 bit	Under investigation
MX-E40 MX-U40	Intel Celeron 1020E 2.2 Ghz – dual core	Windows Embedded Standard 7 32 and 64 bit	
MX-E20 MX-U20	Intel Celeron 1047UE 1.4 Ghz – dual core	Windows Embedded Standard 7 32 and 64 bit	
MX80	Intel Core i7-2710QE	Windows 7 for Embedded Systems, Windows XP	
MX40	Intel® Core™2 Duo Processor P8400	Windows 7 for Embedded Systems, Windows XP	
MX20	Intel® Celeron® Processor T3100	Windows 7 for Embedded Systems, Windows XP	

Laser Marking Systems			
Product	**Processor**	**OS**	**Status**
AREX 2.0 family			
	Intel N450 1.66GHz	Windows XP Embedded SP1	Under investigation
	Intel® Atom™ N455	Windows XP Embedded SP1	
AREX 3.0 family			
	Intel® Atom™ E3825	Windows Embedded Standard 7 32	Under investigation
	Intel® Atom™ N455	Windows Embedded Standard 7 32	
		Windows XP Embedded SP1	
	Intel N450 1.66GHz	Windows XP Embedded SP1	
AREX 20MW			
	Intel® Atom™ E3825	Windows Embedded Standard 7 32	Under investigation
	Intel® Atom™ N455	Windows Embedded Standard 7 32	
VLASE family			
	Intel® Atom™ E3825	Windows Embedded Standard 7 32	Under investigation
	Intel® Atom™ N455	Windows Embedded Standard 7 32	
UNIQ			
	Intel® Atom™ E3825	Windows Embedded Standard 7 32	Under investigation
	Intel® Atom™ N455	Windows Embedded Standard 7 32	
EOX family			
	Intel® Atom™ E3825	Windows Embedded Standard 7 32	Under investigation
	Intel® Atom™ N455	Windows Embedded Standard 7 32	
		Windows XP Embedded SP1	
	Intel N450 1.66GHz	Windows XP Embedded SP1	

Identification Products		
Product	**Processor**	**Status**
DS2100N/DS2400N ETHERNET models	Cortex A8 Eth AM3352 BSP	Under investigation
DS5100	Cortex A8, AM3357 BSP	
DS2100N/DS2400N PROFINET models	Cortex A8, AM3357 BSP	
Axiom/Axiom X	TI TMS320VC5471	Not Impacted
DS8110	TI TM320DM6441	Not Impacted
DX8210	TI TM320DM6441	Not Impacted
DM3610	TI TM320DM6446	Not Impacted
DM3500	TI TMS320C31PQL-60	Not Impacted
AV6010	Freescale i.MX31	Not Impacted
SC5000	TI TM320DM6441	Not Impacted
SC6000		
	Intel® XScale™ Microarchitecture	Not Impacted
	Neuron® Chip Network Processor	Not Impacted
	ARM7TDMI 32-bit Risc Processor	Not Impacted
SC8000		
	AMD –X5-133ADW (Am5x86-P75) Microprocessor	Not Impacted
	VIA Eden ESP 4000 (100 x 4.0) 1.05V Microprocessor	Not Impacted
DM3610	TI TM320DM6446	Not Impacted
Rangefinder	Freescale i.MX31	Not Impacted
Matrix 410N™	TI TMS320DM6435	Not Impacted
Matrix 450N™	TI TMS320DM648	Not Impacted

If your product is not listed here, please contact your Datalogic representative for more information.

ADDITONAL RESOURCES

You can find a comprehensive list of affected computer hardware and software, and the patches issued by vendors here:
https://meltdownattack.com

Following is the link to the Project Zero team that found the vulnerability:
https://googleprojectzero.blogspot.ca/2018/01/reading-privileged-memory-with-side.html

More info from Congatec related to Soredi products:
https://www.congatec.com/en/congatec-ag/spectre.html