Honeywell
THE POWER OF CONNECTED

Cyber Security Update

Security Notification – Processor Vulnerabilities (Spectre & Meltdown) from Safety & Productivity Solutions

BACKGROUND

Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 & CVE-2017-5715) exploit critical vulnerabilities in modern processors. These hardware bugs allow an attacker to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include passwords stored in a password manager or browser, personal identifiable information, photos, emails, instant messages and even business-critical documents. While the vulnerabilities are significant, and proof of concept exploit code has been released, no known exploits have been found in the wild. The key points include:

- Because Meltdown and Spectre impact Intel, AMD, and ARM processors, all types of systems from desktop, to server, to cloud, to IoT and mobile devices are impacted.
- Windows, Linux, and OS X (prior to High Sierra 10.13.2) are all impacted by these vulnerabilities.
- The vulnerabilities do not appear to allow remote access; instead, they are information disclosure vulnerabilities that could allow an attacker to gain information about the target system.
- Exploiting the vulnerability can be done remotely using client-side JavaScript or other typical web-based attack methods.

RECOMMENDED ACTION

Honeywell Safety & Productivity Solutions recommends customers work with their respective service teams to undertake preventative measures to improve the security of their systems, including the following:

- **Keep the Operating System Current**: Unpatched or outdated operating systems and application software are often more susceptible to cyber-attacks, ensure updates are being installed on a timely and regular basis. This vulnerability is directly related to the operating system functionality and therefore is critical address the vulnerability.
- **Security Updates**: Because the vulnerabilities exploit the operating system and certain apps, we are dependent upon receiving security updates from our software partners. We are working diligently with them to provide update as soon as possible. Be sure to monitor our website for further updates on patch availability.
- **Run Only Trusted Applications:** Ensure that devices run only the minimum set of trusted applications that have been thoroughly tested and approved. Ensure programs run with minimal privileges necessary.
- **Anti-Virus**: Where applicable, ensure that anti-virus software is up to date and installed across all assets.
- **Backups**: Ensure appropriate backups and system restoration procedures are in place, with copies of the most recent backup stored in an offline/disconnected state to reduce infection susceptibility.

IMPACTED PRODUCTS – 19 April 2018

Productivity Products		
Product Name	Software	Status
Dolphin CT60	Android 7.1	**Fix Available in 83.00.03 or 84.00.03 or Later**
Dolphin CT50 Dolphin 75e	Android 6.0	**Fix Available in 68.01.15, 69.01.15, 70.01.15, 71.01.15**
	Android 4.4	Not Impacted
	Windows 8.1 EH	Upgrade to Windows 10 IoT Mobile
	Windows 10 IoT Mobile	Patch from Microsoft Available
CN51	Android 6.0	Not Impacted
	Android 4.2	Not Impacted
	Windows WEH 6.5	**Mitigate w/ Security Controls – See Additional Resources**

Honeywell
THE POWER OF CONNECTED

Cyber Security Update

Productivity Products		
Product Name	Software	Status
CN75, CN75e, CK75	Android 6.0	Not Impacted
	Windows WEH 6.5	**Mitigate w/ Security Controls – See Additional Resources**
Thor VM3	Windows 10	Patch from Microsoft Available
	Windows 7	Patch from Microsoft Available
	Windows WES 7	Patch from Microsoft Available
	Windows WEC7	**Upgrade to Windows WES 7**
Thor VM2	Windows 7	Patch from Microsoft Available
	Windows WES 7	Patch from Microsoft Available
	Windows CE 6	**Not Impacted**
	Windows WES 2009	Upgrade to Windows WES 7 or Windows 7
Thor VM1 CV41	Windows CE 6	**Not Impacted**
	Windows WES 2009	**Mitigate w/ Security Controls – See Additional Resources**
CV31	Windows WEC7	**Not Impacted**
CV61	Windows 7	Patch from Microsoft Available
	Windows XP	Upgrade to Windows 7
D99 Series	Windows WEH 6.5	**Mitigate w/ Security Controls – See Additional Resources**
CK3R, CK3X	Windows WEH 6.5	**Mitigate w/ Security Controls – See Additional Resources**
CN70, CN70e, CK70, CK71	Windows WEH 6.5	**Mitigate w/ Security Controls – See Additional Resources**
Tecton	Windows WEH 6.5	Not Impacted
Dolphin 6110	Windows CE 6	**Not Impacted**
	Windows WEH 6.5	**Not Impacted**
Dolphin 6510	Windows CE 6	**Mitigate w/ Security Controls – See Additional Resources**
Dolphin 70e Dolphin 60s Dolphin7800	Windows WEH 6.5	**Mitigate w/ Security Controls – See Additional Resources**
Workflow Solutions		
Talkman A500	Windows CE 6	Upgrade to Windows WEC7
	Windows WEC7	Under Investigation
Talkman A710 Talkman A720 Talkman A730	Windows WEC7	Under Investigation

ADDITIONAL RESOURCES

- **Honeywell Network & Security Guide for Windows Mobile 6.5 –** https://www.honeywellaidc.com/en/-/media/en/files-public/security-notices/windows-mobile-6_5-network-security-guide-en.pdf
- **Honeywell Network & Security Guide for THOR VM3** – https://www.honeywellaidc.com/-/media/en/files-public/technical-publications/computers/thor-vm3/VM3-WIN-ENUS-ZY.pdf
- **Vulnerability Note VU#584653** https://www.kb.cert.org/vuls/id/584653
- **National Vulnerability Database CVE-2017-5753** https://nvd.nist.gov/vuln/detail/CVE-2017-5753
- **National Vulnerability Database CVE-2017-5754** https://nvd.nist.gov/vuln/detail/CVE-2017-5754
- **National Vulnerability Database CVE-2017-5715** https://nvd.nist.gov/vuln/detail/CVE-2017-5715
- **Meltdown & Spectre Website:** https://meltdownattack.com/