Processor Vulnerabilities (Meltdown and Spectre) Update from Honeywell Security and Fire

Cyber Security researchers have recently identified a set of industry-wide security vulnerabilities in the Central Processing Units (CPUs) of most computing systems related to an anomaly in the CPU hardware itself.

These vulnerabilities, Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 & CVE-2017-5715) exploit the design of the CPU optimization functions potentially allowing an attacker to steal data which is currently processed on the computer. While applications are typically not permitted to read data from other programs, a malicious attacker could exploit Meltdown and/or Spectre to gain secrets stored in the memory of other running programs. This may include passwords, cryptographic keys, personally identifiable information, photos, emails, etc. While the vulnerabilities are significant, and proof of concept exploit code has been released, no known exploits have yet been found in the wild.

The impact is that all modern computers and their variants housing an Intel, AMD, Apple, and any CPU chip based on the ARM architecture may be vulnerable.

More details regarding these vulnerabilities (including technical details and manufacturer security advisories) may be obtained from the links below.

Honeywell takes the security of our customers and products seriously. As a leading global technology company, some of our products utilize CPUs identified in these recent disclosures and could potentially be affected by recently released Spectre / Meltdown exploits. Upon learning about this CPU issue, we began a company-wide product review to determine which of our products / solutions are affected, and

what corrective actions are necessary. We are committed to communicating with customers as quickly as possible about any systems that are affected, and the actions required to mitigate the vulnerabilities.

IMPACTED PRODUCTS

To view a list of impacted products, please see the appendix on the last pages of this document. This not only lists affected products, but also whether patches are available and what effect they have on the performance of the product.

These events highlight the importance for organizations to ensure that their systems are up-to-date with the most current software versions and updates, and properly maintained and monitored. Prevention is often the best protection.

RECOMMENDED ACTION

Honeywell recommends that customers work with their respective service teams to undertake preventative measures to enhance the security of their security and fire systems, including the following:

- **Security Updates:** Operating system, firmware, and application updates are intended to mitigate these attacks. Note that in many cases, the software fixes for these vulnerabilities may have a negative effect on system performance. These effects on performance are listed in the attached appendix. As with deploying any software updates, be sure to prioritize and test updates as necessary. Updates to affected devices should be promptly installed as/when they become available from manufacturers. Users should check with their hardware manufacturer for guidance on patch availability and installation.
- **Anti-Virus:** Always ensure that anti-virus software is up to date and installed across all assets.
- **Keep 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.
- **Backups:** Ensure appropriate backups and system restoration procedures are in place, with copies of the most recent backup stored in an offline location.
- **Awareness:** Educate system users to take care when opening emails and attachments. Ensure building control system servers and workstations are not being used for email access or general web browsing, and logically separated if running on a shared network. Inform and educate system users on how to identify scams, malicious links, and social engineering attempts.
- **Report concerns:** Promptly report any unusual system activity or unplanned disruption to your service team.
- **Ongoing vigilance:** Work with your service team to review service maintenance activities and frequency, and develop an appropriate cyber security improvement plan. Additional activities may include undertaking a proactive cyber security health review of your Honeywell systems.

ADDITIONAL RESOURCES / TECHNICAL REFERENCES

- **Vulnerability Note VU#584653** https://www.kb.cert.org/vuls/id/584653
- **Meltdown & Spectre Website:** https://meltdownattack.com/

DISCLAIMER

This publication is provided as general advice only as part of our commitment to product security and customer service, but it is not a substitute for site specific professional advice appropriate for your circumstances.