Hanwha Techwin
6, Pangyo-ro 319 beon-gil, bundang-gu, Seongman-si, Gyeonggi-do, 463-400 Rep. of KOREA
TEL 82.70.7147.8753 FAX 82.31.8018.3740 www.hanwha-security.com

January 16, 2018 Hanwha Techwin

# "Meltdown", "Spectre" vulnerabilities Report

## 1. 취약점 확인

- CPU의 명령어 실행순서 변경이 잘못되거나 실행순서 예측이 실패 했을 경우에, 저장되는 캐시 메모리 값이 공격자의 사이드 채널 공격(ex, Cache timing Attack)에 의해 유출 될 수 있음
  - ✓ Meltedown(CVE-2017-5754) : Intel 프로세서에서 확인되는 취약점으로, 사용자 공간에서 커널 메모리 공간에 존재하는 정보에 접근(유출) 할 수 있음
  - ✓ Spectre(CVE-2017-5753 & CVE-2017-5715) : Intel, ARM 및 AMD 프로세서에 확인되는 취약점으로, 다른 어플리케이션 메모리 공간에 존재하는 정보에 접근(유출) 할 수 있음

## 2. 한화테크윈 제품 영향도 분석

- 당사에서 개발한 일부 카메라/저장장치/콘트롤러의 경우 ARM사(Cortex 계열)의 CPU를 사용하고 있으며, 이를 적용한 일부 제품에 대해 Spectre 취약점이 존재함

* Meltedown 취약점은 해당사항 없음

| 제조사 | 칩명 | CPU | Meltdown | Spectre |
|---|---|---|---|---|
| Hisilicon | Hi3559A | CortexA73 | X | O |
| | Hi3531A | Cortex A9 | X | O |
| | Hi3521/3520A | Cortex A9 | X | O |
| | Hi3535 | Cortex A9 | X | O |
| | Hi3536 | Cortex A17 | X | O |
| Amabarella | S2LM33 | CortexA9 | X | O |
| HTW | WN3 | CortexA8 | X | O |
| TI | DM8127 | Cortex A8 | X | O |

[취약점이 확인되는 CPU 리스트]

- 단, 악의적인 공격코드가 침투되거나 임의의 코드를 실행시킬 수 없는 제한된 어플리케이션 실행 환경으로, Spectre 취약점이 발생하지 않음

## 3. 결론

- 당사 제품(카메라/저장장치/콘트롤러)에 대한 Spectre 취약점 영향도가 없으므로, 별도의 대응 계획은 없음