WSEC Security Response

Processor Reading privileged memory with a side-channel (MELTDOWN/SPECTRE)

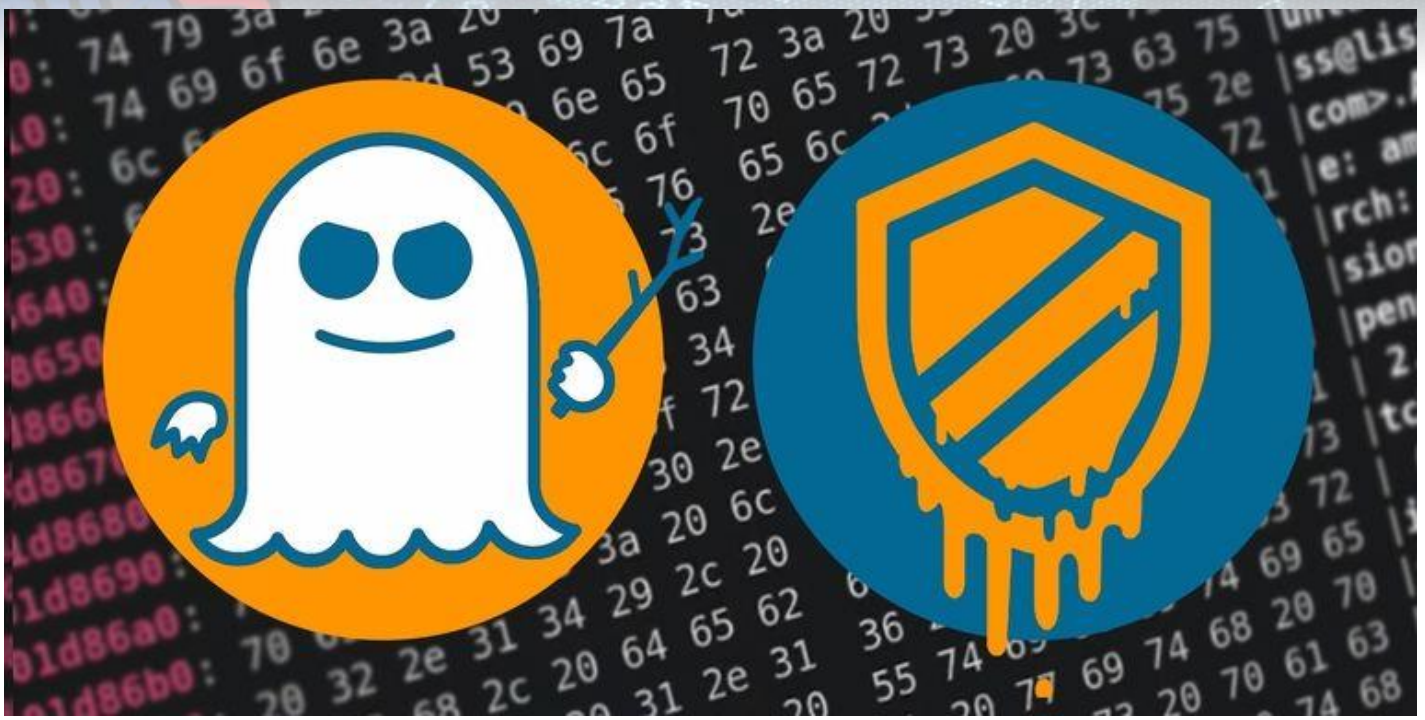
WSEC(Wins Security Emergency Center)

Version 1 – 2018-01-05

구글 프로젝트 Zero 팀에 의해 발표된 Prcessor 메모리 유출 취약점인 Meltdown과 Spectre는 Intel CPU 뿐 아니라 AMD,ARM 등의 모든 CPU 프로세스에 해당한다.
CPU 프로세스의 속도 경쟁에 따른 구조적 결함으로 벤더사의 패치를 실시한다 해도 기존 성능의 30%내외 퍼포먼스 손실이 발생할 수 있다.

Visit Our Homepage
http://securecast.co.kr

Visit Our Blog
http://www.wins21.co.kr/blog/blog.html



최신 프로세서에서 Meltdown 과 Spectre 라는 새로운 취약점 2 개가 발견되어 악성 프로그램이 다른 프로그램의 메모리에서 정보를 훔칠 수 있습니다. 즉, 악성 프로그램이 암호, 계정 정보, 암호화 키 또는 이론적으로 프로세스의 메모리에 저장된 모든 것을 훔칠 수 있습니다.

공급 업체는 고객이 Spectre 또는 Meltdown 및 서비스 상태로부터 자신을 보호 할 수있는 방법에 대한 정보를 공개하기 시작했습니다. 관련 CVE 는 CVE-2017-5753, CVE-2017-5715 및 CVE-2017-5754 입니다.

그러나 소프트웨어 업데이트가 이러한 취약점을 완전히 해결할 수는 없다는 점에 유의해야합니다. 랩톱이나 컴퓨터에 최신 BIOS / 펌웨어 업데이트가 설치되어 있는지 확인하는 것도 중요합니다.

Meldown, Spectre 취약점은 로컬 취약점으로 User 권한으로 실행된 파일이 메모리 사이드채널의 정보를 유출합니다. 즉 실제적인 공격이 발생할 경우 다음과 같은 Case 가 있을 수있습니다.

Case 1) 클라우드 시스템에 침입한 공격자가 Meldown, Spectre 취약점을 이용해 메모리 덤프 후 클라우드의 모든 계정정보를 열람 탈취 가능

Case 2) 업데이트 서버, 중앙 관리 서버 등의 신뢰받는 소프트웨어서버를 공격하는 supply chain attack 을 통해 조직 정보 탈취

Case 3) Doc,Xls,Hwp 와 같은 문서 파일에 취약점 파일을 삽입 후 웹/메일을 통해 유포 후 사용자 PC 의 정보를 탈취 <- 이 경우는 공격자의 직접적인 개입이 어렵기 때문에 공격 성공이 매우 어려움

☞ **1 차적인 접근 권한 탈취가 이뤄진 이후 로컬에서 공격자가 메모리 정보를 유출하는 방식의 공격형태로 클라우드, 중앙관리 시스템 DB 와 같은 서버 기반과 같이 메모리 상에 다양한 정보가 존재하는 서버가 위험군으로 분류 가능**

Meldown (rogue data cache load (CVE-2017-5754))

Meltdown 은 사용자 응용 프로그램과 운영 체제 간의 Isolation 규칙을 우회합니다. 이 공격은 프로그램이 다른 프로그램과 운영 체제의 메모리에 접근해 메모리 정보를 유출할 수 있으며, 패스워드와 같은 기밀 정보 유출이 가능합니다.

Spectre (branch target injection (CVE-2017-5715) / bounds check bypass (CVE-2017-5753))

Spectre 는 여러 응용 프로그램 사이의 Isolation 규칙을 우회합니다. 이를 통해 공격자는 취약점이 존재하지 않은 프로그램일지라도 메모리 유출을 통해 패스워드와 같은 기밀정보를 획득할 수 있습니다.

History

오류 발견 1 일차

레지스터에 의하면 마이크로소프트는 다음 주에 있을 '패치 튜즈데이'를 통해 해당 오류에 대한 패치를 배포할 예정이고, 리눅스 개발자들은 온라인 커뮤니티를 통해 공개적으로 픽스 작업을 진행 중에 있다. 하지만 윈도우든 리눅스든 업데이트 이후 시스템 속도가 5~30% 떨어질 것으로 예상된다고 한다. 최신 인텔 칩일수록 느려지는 정도가 덜 할 것으로 보인다.

하지만 해당 보도에는 오류 자체에 대한 설명은 없었다. 인텔과 마이크로소프트 모두 인터뷰 요청에 응답을 하지 않거나 거절한 상태였다. 그 시점에서 보안 전문가 댄 카민스키(Dan Kaminsky)는 "오류에 대한 세부 사항은 밝히지 않은 채 패치 후 속도가 느려진다거나 이런 저런 영향이 있을 거라는 식의 내용부터 전달하는 건, 순서가 바뀐 거 아닌가"하는 의문을 제기했다.

지금까지 알려진 바에 의하면 이 오류는 1) 커널과 관련이 있는 것으로 현존 수십 억대의 컴퓨터 시스템에 영향을 미치며, 2) 웹 브라우저 내 자비스크립트를 포함한 여러 애플리케이션을 통해 커널 메모리의 보안 영역에 접근할 수 있게 해준다. 보안 업체 소포스(Sophos)의 보안 분석가인 폴 더클린(Paul Ducklin)은 "커널은 원래 민감한 영역을 사용자 영역으로부터 분리해, 사용자가 사용하는 프로그램이 안전한 공간 안에서만 안전하게 기능을 발휘할 수 있도록 하는 것"이라며 "여기서 문제가 발생했다면, 심상치 않은 것"이라고 말했다.

그래서 새롭게 발표될 리눅스 패치는 커널 페이지 테이블 아이솔레이션(Kernel Page Table Isolation, KPTI)이라는 것을 활용해 커널 메모리와 사용자 프로세스를 완전히 구분해놓을 전망이다. 더클린은 이러한 패치 소식에 "여러 명이 공동으로 사용하는 컴퓨터 시스템에 알맞은 패치"라며 "특히 가상기기를 여러 개 운영하는 서버 등에 적합할 것"이라고 평했다.

한편 엔드포인트 기기나 가전 장비는 공격 받을 가능성이 그리 높아 보이지 않는다고 한다. 취약점을 익스플로잇 하려면 코드를 실행시켜야만 하기 때문인데, 데스크톱이나 서버와 같은 시스템이 아니라면 코드 실행이 용이하지 않기 때문이다. "멀티유저 빌드 서버나, 하나의 물리 하드웨어 안에 다수의 가상기기를 운영하면서 여러 고객들에게 호스팅 서비스를 제공하는 컴퓨터의 경우, 이 커널 취약점은 중대한 문제가 됩니다. 논리적 구분을 무의미하게 만들 수 있는 것이니까요."

최근 인텔은 보안 전문가들의 입에 자주 오르내리는 기업이 되었다. 지난 해 5 월에는 인텔 칩 내 액티브 매니지먼트 테크놀로지(Active Management Technology, AMT) 펌웨어에서 치명적인 권한 상승 오류가 발견되는 바람에, 인텔 칩 사용자들이 발칵 뒤집히기도 했다. 이 취약점의 경우 보안 업체 엠베디(Embedi)에서 발견한 것으로, 공격자들이 아무런 인증 절차를 거치지 않고 AMT 기능을 조작할 수 있도록 해줬다. 즉 원격에서 OS 를 삭제하거나 재설치할 수 있으며, 마우스와 키보드 조작까지도 가능하도록 해주는 취약점이었던 것이다.

그러더니 작년 가을, 인텔은 다시 한 번 마이크로프로세서 내 취약점을 패치했다. 이 취약점은 공격자들이 기계 깊숙이 숨어서 프로세스를 통제하고 데이터에 접근하도록 해주는 것이었다. 얼마나 깊게 숨게 해주는지, 랩톱이든 워크스테이션이든, 서버든 공격자가 한 번 침투하면 전원이 꺼져있어도 공격이 가능했다고 한다. 이 취약점은 또 다른 보안 업체 포지티브 테크놀로지스(Positive Technologies)가 인텔의 매니지먼트 엔진(Management Engine, ME) 11 시스템에서 처음 발견했다.

2015 년부터 출시된 인텔 칩들이 이 이슈에 해당됐다.

AMT 와 ME 에 이어 이번엔 '설계 오류'까지, 인텔은 단기간 내 세 번의 보안 이슈를 만든 주인공이 됐다. 하지만 아직도 그 오류의 기술적인 세부 사항은 알려지지 않고 있다. 더클린은 포스팅을 통해 "이번에 밝혀진 오류는 수년 동안 존재해왔으며, 문건으로도 여러 차례 공개된 것"이라고 설명한다. "즉 '패닉'에 빠질 만큼 심각한 건 아니라는 겁니다. 하지만 인텔의 패치 소식을 주시하고 있다가 즉각 업데이트를 진행할 필요는 있습니다. 1 월 안에는 나올 전망입니다."

아마존 EC2 와 마이크로소프트 애저, 구글 컴퓨트 엔진 등 클라우드 서비스들도 이번에 발견된 인텔 설계 오류의 영향권 아래 있다는 소식도 있었다. 보안 업체 벡트라(Vectra)의 보안 분석 책임자인 크리스 모랄레스(Chris Morales)는 "아마존이 방금 대규모 보안 업데이트가 있을 예정이며, EC2 를 이번 주 금요일 리부트 한다는 내용의 통지서를 보내왔다"고 설명한다.

"이번 인텔 오류와 관련된 조치의 일환이라고 보이는데, 맞다면 클라우드까지 리부트시킬 정도로 심각한 오류가 우리의 시스템들 안에 있음을 시사합니다." 사실 '클라우드가 리부트 한다'는 건 우리가 흔히 들을 수 있는 통보문은 아니다. 그것도 아마존에서부터라니. 그래서 모랄레스는 "Y2K 때가 생각날 정도"라고 말한다.

2 일차

드디어 구글의 프로젝트 제로 팀과 보안 업체 사이버러스(Cyberus), 그라즈기술대학, 펜실베이니아대학, 메릴랜드대학, 애들레이드대학, 보안업체 데이터 61(Data61)의 연구원들이 IT 업계를 들썩였지만 공개되지 않은 인텔 취약점의 정체를 공개했다. 이 취약점은 시스템 퍼포먼스 최적화와 관련된 프로세서 내에 존재하며, 익스플로잇 할 경우 민감한 시스템 메모리를 공격자가 읽을 수 있게 해주는 것으로 밝혀졌다. 인텔, AMD, ARM 에서 만든 CPU 들이 이 취약점을 내포하고 있을 가능성이 높다고 한다.

이 취약점을 익스플로잇 하는 공격은 크게 두 가지로 각각 멜트다운(Meltdown)과 스펙터(Spectre)라고 불린다. 데스크톱, 랩톱, 모바일, 클라우드 환경에서 공격이 성립 가능하다. 한 클라우드 서비스 내 여러 고객의 정보를 훔쳐가는 것도 가능하다는 뜻이 된다.

먼저 멜트다운은 사용자 애플리케이션들을 통해 OS 메모리로부터 정보를 빼돌리게 해주는 공격이다. OS 메모리뿐만 아니라 다른 애플리케이션에 저장된 정보들도 공격 대상이 될 수 있다. 구글 전문가들은 다음과 같이 권고한다. "지금 사용하고 있는 컴퓨터에 취약점을 가지고 있는 칩이 꽂혀있다면, 그리고 OS 가 최신화 되지 않았다면, 그 컴퓨터로는 민감한 작업을 하지 않는 것이 안전합니다. 개인 컴퓨터도 그렇지만 클라우드 환경에 있더라고 마찬가지입니다."

1995 년 이후 만들어진 인텔 프로세서들은 대부분 멜트다운 공격에 취약하다. 2013 년 이전에 출시된 인텔 아이테니엄(Intel Itanium)과 인텔 아톰(Intel Atom)은 예외다. 인텔 외 다른 회사의 프로세서에서는 멜트다운 취약점이 발견된 바 없다.

반면 스펙터는 애플리케이션들이 기밀이나 민감한 정보를 공유하도록 강제하는 공격이다. 멜트다운보다 성공시키기가 어렵다. 데스크톱, 랩톱, 클라우드 서버, 스마트폰 등에 사용되는 인텔, AMD, ARM 프로세서들이 스펙터 공격에 취약하다. 멜트다운이나 스펙터나 메모리 영역에서부터 민감한 정보를 빼내는 것을 목적으로 하고 있지만 특이하게도 널리 알려진 보안 실천 사항들을 준수하면 스펙터에 당할 확률이 더 높아진다고 한다.

현재까지 인텔의 이 '설계 오류'로 인한 실제 피해 사례가 발생하지는 않은 것으로 보인다. 하지만 이제 2 일차라 확신할 수는 없는 부분이라고 전문가들은 말한다.
사실 전문가들은 이 취약점을 1 월 9 일에 공개하기로 했다고 한다. 구글이 이를 어기고 발표한 것이다. 그 이유에 대해 구글 보안 엔지니어인 맷 린턴(Matt Linton)은 "매체와 보안 커뮤니티 내에 추측성 소식들이 난무해져 가는 게 더 위험해 보여서"라고 밝혔다.
침묵을 지키던 인텔은 "해당 취약점을 조사해본 결과 데이터를 조작하거나 삭제하는 권한까지 공격자에게 주지 않는다"고 발표했다. 또한 "시스템이 느려질 것이라고는 하지만, 일반적인 컴퓨터 사용 환경에서 크게 체감되지 않을 것"이라고도 말했다.
구글의 발표 내용은 여기(https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html)서 열람이 가능하다.

보안뉴스 기사 발췌

<출처 : http://m.boannews.com/html/detail.html?idx=65894 >

취약점 점검 및 업데이트 방법

Microsoft 는 PC 가 업데이트를 제대로 설치했는지 또는 추가 펌웨어 업데이트가 필요한지 확인하는 데 사용할 수있는 Powershell one-liners 제공합니다.

PowerShell 을 시작할 때 필요한 모듈을 설치할 수 있도록 관리자 권한으로 시작해야합니다.

아래의 Powershell 명령은 Meltdown 및 Spectre 결함을 테스트하기 위해 Powershell 모듈을 다운로드하고 설치합니다.

```
Install-Module SpeculationControl
```

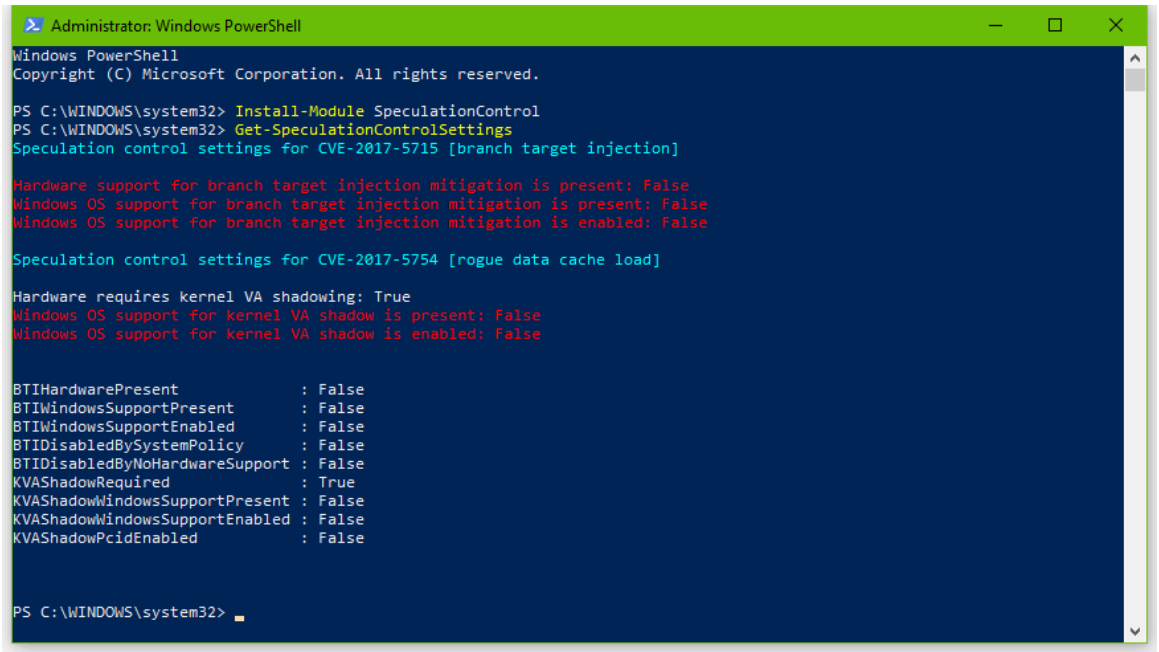
명령을 실행하고 실행 오류가 발생하면 Powershell 실행 정책을 조정해야 할 수 있습니다. 다음 명령을 실행하십시오.

```
Set-ExecutionPolicy Bypass
```

이제 실제로 시스템을 검사하는 두 번째 Powershell 명령을 실행할 수 있습니다.

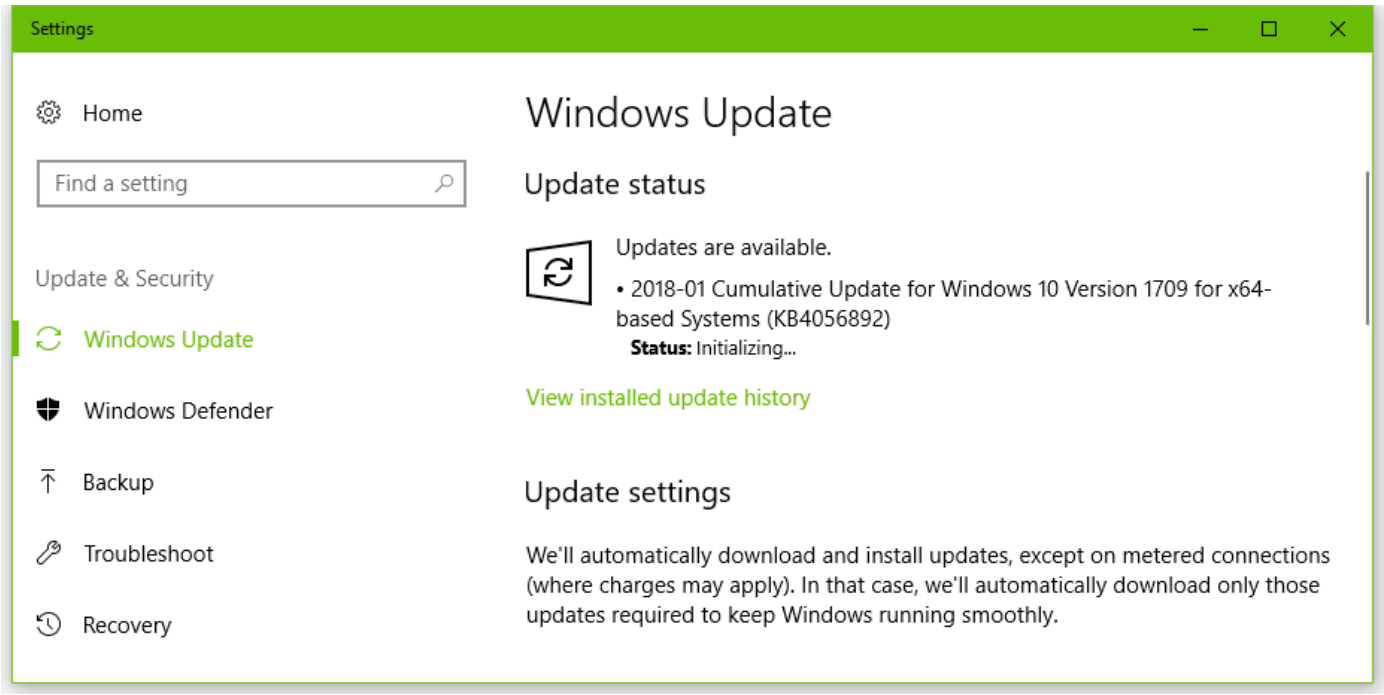
```
Get-SpeculationControlSettings
```

Google 은 모든 CPU 가 Meltdown 및 Spectre 결함에 취약하지는 않지만 결과가 빨간색으로 표시된 텍스트가 많으면 CPU 와 OS 가 이러한 공격에 취약하다는 것을 알려줍니다. 가장 가능성이 높습니다.



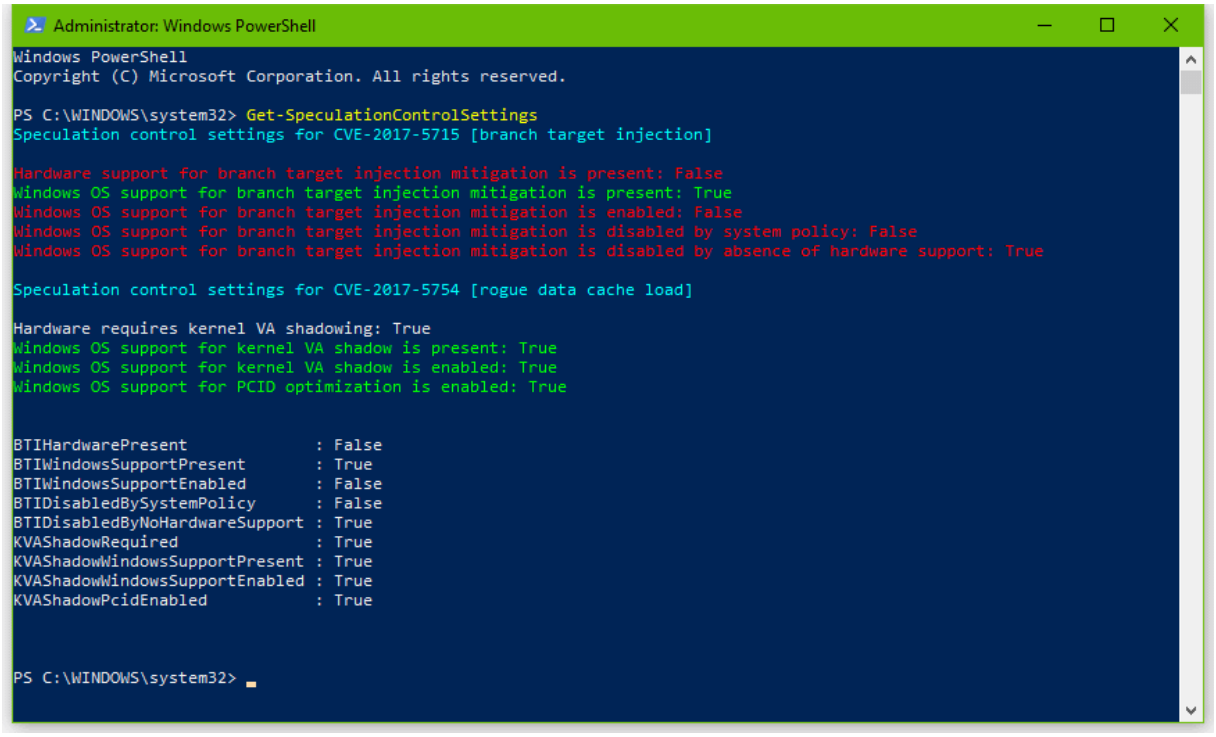
[그림.1] Powershell 실행 화면

다음 단계는 Meltdown / Spectre 패치를받을 때까지 "업데이트 확인"버튼을 누르는 것입니다. "문제가있는"안티 바이러스 소프트웨어를 사용하는 일부 사용자의 경우 며칠이 걸릴 수 있습니다.



[그림.2] Windows Update 실행 화면

업데이트가 끝나면 Get-SpeculationControlSettings 를 다시 실행해야합니다. 가능한 시나리오는 두 가지입니다. 가장 일반적인 시나리오는 다음 결과입니다.



[그림.3] Meltdown 버그 패치완료 / Spectre 버그 패치 미완료

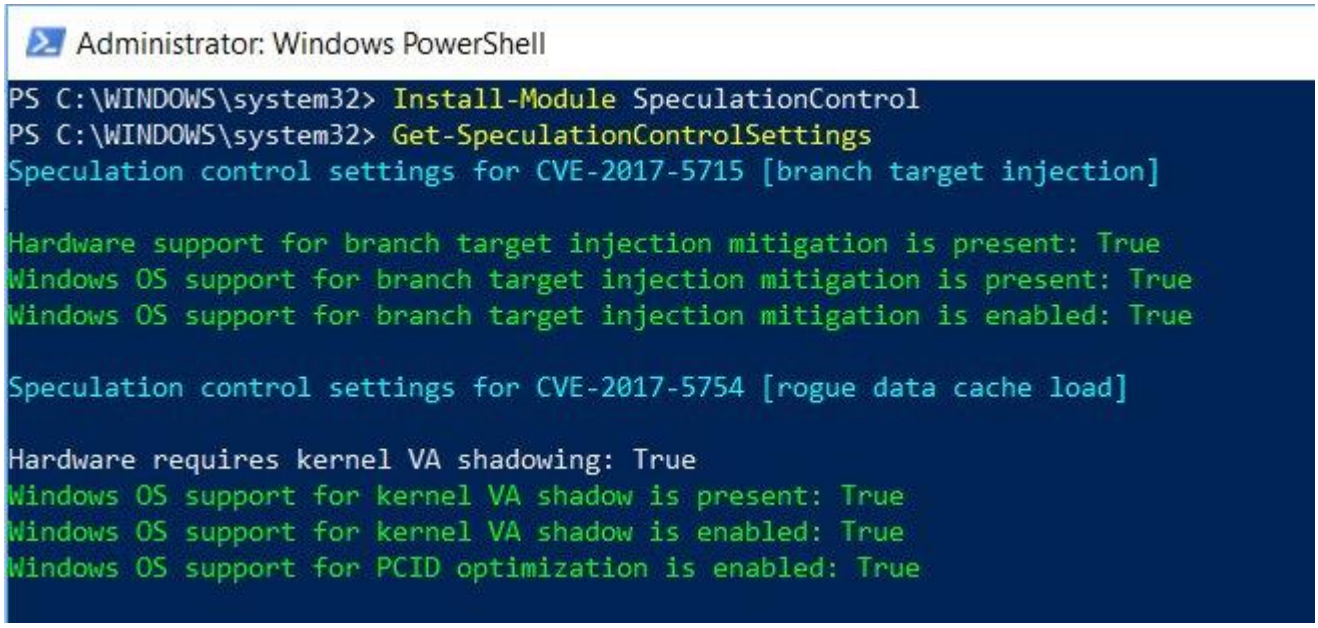
[그림 3]은 시스템이 Meltown 버그에 대한 패치를 받았지만 Spectre 버그에 대한 불완전한 패치를 받았음을 의미합니다.

구글이 어제 발표 한 바와 같이, 스펙터는 악용하기가 어렵지만 패치하기가 더 어렵습니다.

빨간색 텍스트는 추가 칩셋 펌웨어 업데이트가 필요하다는 것을 의미합니다. 마이크로 소프트와 구글에 따르면 완벽한 Spectre 패치를 위해서는 OEM 업체들이 윈도우 OS 레벨의 Spectre 패치를 완성하기 위해 추가 펌웨어 업데이트를 사용자들에게 제공해야 하는데 과거 버전의 PC 의 경우 일부 OEM 에서 이 펌웨어 업데이트를 제공하지 않을 수 있습니다. 즉, 불완전한 Spectre 패치가 진행 될 수 있음을 유념하십시오.

랩톱 / 데스크톱 / 서버 공급 업체가 추가 칩셋 펌웨어 업데이트를 제공 한 경우 해당 공식 사이트에서 업데이트를 가져와 설치하고 패치를 완료 할 수 있습니다.

모든 것이 정상이면 모든 검사는 녹색 색상의 텍스트로 표시됩니다.



[그림.4] Meltdown 버그 패치완료 / Spectre 버그 패치 완료

취약한 버전

Meldown (rogue data cache load (CVE-2017-5754))

- **1995 년 이후의 모든 프로세서 (2013 년 이전 Intel Itanium 및 Intel Atom 제외)**

Spectre (branch target injection (CVE-2017-5715) / bounds check bypass (CVE-2017-5753))

- **Intel, ARM,AMT 등 모든 프로세스**

벤더사별 권고, 주의사항, 업데이트

Amazon

Amazon 은 Amazon AWS 서비스가 Meltdown and Spectre 의 영향을받는 방법에 대한 정보를 제공하는 보안 공지를 발표했습니다.

Meltdown and Spectre 취약점은 인텔, AMD, ARM과 같은 최신 프로세서 아키텍처에서 서버, 데스크톱 및 모바일 장치 전반에 걸쳐 20 년 넘게 존재해온 취약점입니다. Amazon EC2 인스턴스 중 몇몇을 제외하면 이미 보호되어 있습니다. 나머지 인스턴스는 관련 인스턴스 유지 보수 알림과 함께 다음 몇 시간 내에 완료됩니다.

AWS의 업데이트가 기본 인프라를 보호하는 동안 이러한 문제로부터 완벽하게 보호하려면 고객은 인스턴스 운영 체제에도 패치를 적용해야합니다. Amazon Linux에 대한 업데이트가 제공되었으며,이 게시판과 관련된 다른 AWS 관련 지침과 함께 기존 인스턴스 업데이트 지침이 아래에 추가로 제공됩니다.

Amazon 전체 보안 공지 (https://aws.amazon.com/security/security-bulletins/AWS-2018-013/)

AMD

AMD 는 Spectre 실행 취약점에 취약하지 않다고 공식 권고문을 공개하지 않았습니다.
아래는이 보도 자료의 표입니다.

	Google Project Zero (GPZ) Research Title	Details
Variant One	Bounds Check Bypass	Resolved by software / OS updates to be made available by system vendors and manufacturers. Negligible performance impact expected.
Variant Two	Branch Target Injection	Differences in AMD architecture mean there is a near zero risk of exploitation of this variant. Vulnerability to Variant 2 has not been demonstrated on AMD processors to date.
Variant Three	Rogue Data Cache Load	Zero AMD vulnerability due to AMD architecture differences.

[그림.5] AMD 보도자료 (https://www.amd.com/en/corporate/speculative-execution)

AMD 프로세서는 커널 페이지 테이블 격리 기능이 보호하는 유형의 공격을받지 않습니다. AMD 마이크로 아키텍처는 추측 적 참조를 포함하여 더 적은 권한 모드에서 실행될 때 높은 권한의 데이터에 액세스하여 페이지 오류가 발생할 메모리 참조를 허용하지 않습니다.

X86_FEATURE_PTI가 설정되어 있는지 여부를 제어하는 X86_BUG_CPU_INSECURE 기능을 설정하지 않으면 AMD 프로세서에서 기본적으로 페이지 테이블 격리를 비활성화합니다.

AMD 의 소프트웨어 엔지니어 Tom Lendacky 답변 (https://lkml.org/lkml/2017/12/27/2)

Android

Android 팀은 2018 년 1 월 게시판에 취약점 대응현황을 업데이트했습니다.

CVE-2017-5715, CVE-2017-5753 및 CVE-2017-5754 는 프로세서의 Spectre 와 관련된 일련의 취약점을 공개했습니다. Android 는 모든 ARM 기반 Android 장치에서 권한이 없는 정보 유출을 허용하는이 취약점을 탐지하지 못합니다.

추가 보안 기능을 제공하기 위해 게시판에 포함 된 CVE-2017-13218 의 업데이트는 high-precision timers 에 대한 액세스를 줄여 주므로 side channel 공격 (예 : CVE-2017-5715, CVE-2017-5753 및 CVE-2017-5754)을 제한하는 데 도움이됩니다. ARM 프로세서의 알려진 모든 변형에 적용 할 수 있습니다.

Android 사용자는 사용 가능한 보안 업데이트를 기기에 적용하는 것이 좋습니다. 자세한 내용은 Google 보안 블로그(https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html) 를 참조하십시오.

Android 보안공지 (https://source.android.com/security/bulletin/2018-01-01)

Anti-Virus 벤더업체

Microsoft 는 이번 업데이트로 인한 잠재적인 블루 스크린의 오류를 피하기 위해 호환되지 않는 바이러스 백신 소프트웨어가 있는 시스템에서 업데이트 설치를 차단하기로 결정했습니다.

위와 같은 결정으로 각 벤더사는 긴급으로 호환성 여부 체크 및 Windows 인스턴스에서 수정 사항을 테스트하고 필요한 레지스트리 키를 설정하는 업데이트를 실행했습니다.

다음 표는 각 벤더 사별 윈도우 업데이트에 따른 대응 현황입니다.

				Last update: 4th January 2018 @10.44pm GMT
Vendor	**Product**	**Sets registry key**	**Supported**	**Comment**
AVAST		Y	Y	Fix pushed yesterday to customers
Avira		Y	Y	Now fixed
BitDefender		**N**	N	Fix this evening or tomorrow
Carbon Black		**N**	N	Assessing impact
Cisco	AMP	**?**	?	No statement from vendor so far
CrowdStrike	Falcon	**N**	Y	Registry key change scheduled for Monday
Cylance	PROTECT	**N**	N	Manual registry key setting
Cyren	F-PROT	**N**	N	Working on a fix, cannot set registry key thru usual update
EMSI	Anti-Malware	Y	Y	Now fixed
Endgame		**N**	Y	Manual registry key setting
ESET		Y	Y	
F-Secure	SAFE	Y	Y	Update out now. Legacy products tomorrow.
G-DATA	Antivirus	**N**	N	
Kaspersky		Y	Y	
Malwarebytes	Anti-Malware	Y	Y	Fixed.
McAfee	Endpoint Protection	**N**	Y	Registry key change due soon
Microsoft	Windows Defender	Y	Y	
Palo-Alto	TRAPS	**N**	N	Advisory doesn't say if TRAPS works with patch or sets key
SentinelOne	EPP	**N**	Y	Manual registry key setting
Sophos	Anti-Virus and Central	**N**	Y	Sophos now plan to push registry key update tomorrow
Symantec	Endpoint Protection	Y	Y	Fix in Eraser Engine 117.3.0.359
Trend Micro		**N**	See link	
VIPRE	Endpoint Security	**N**	N	Fix under testing
Webroot		**N**	Y	Manual registry key setting

[그림.6] Anti-Virus 벤더사별 MS 대응 현황

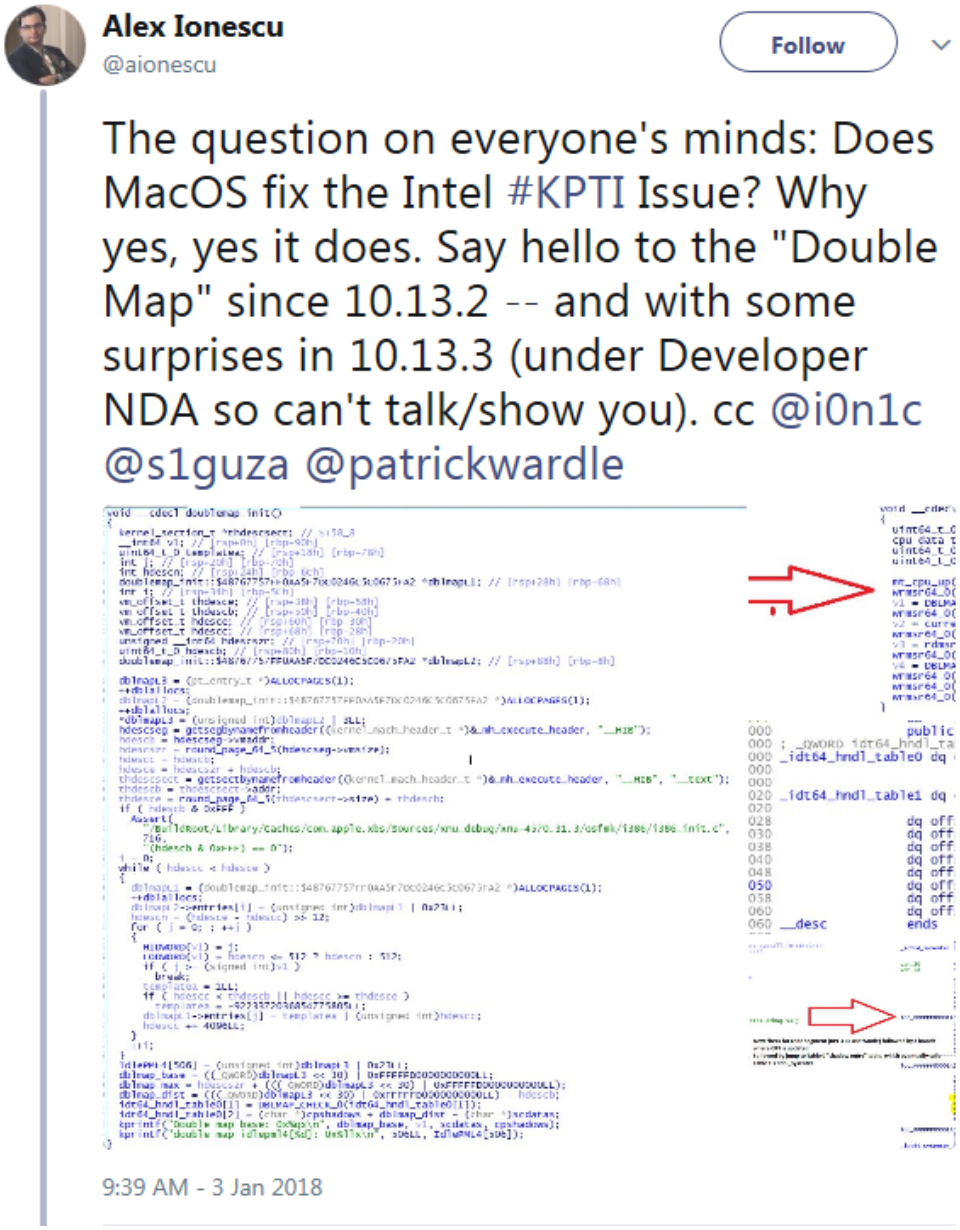
(https://docs.google.com/spreadsheets/u/2/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/htmlview)

1월 4일자 대응 현황 이며, MS에 대응 되지 않는 백신을 사용하는 시스템은 MS의 CVE-2017-5715, CVE-2017-5753 및 CVE-2017-5754 보안업데이트를 받을 수 없습니다.

Apple

현재 애플은 공식적인 답변을 발표하지 않았습니다.

Windows 내부 전문가인 Alex Ionescu 는 다음과 같이 트위터를 통해 의견을 게진했습니다.



[그림.7] <출처 : https://twitter.com/aionescu/status/948609809540046849/photo/1?ref_src=twsrc%5Etfw&ref_url=https%3A%2F%2Fwww.bleepingcomputer.com%2Fnews%2Fsecurity%2Flist-of-meltdown-and-spectre-vulnerability-advisories-patches-and-updates%2F >

ARM

ARM 은 Meltdown 및 Spectre 공격에 취약한 ARM 프로세서 버전별 취약정보를 상세 기재 했습니다.

● Android를 실행중인 경우 지원되는 커널 버전에 대한 자세한 내용은 Google에 문의하십시오.
● 다른 OS를 실행중인 경우 자세한 내용은 OS 공급 업체에 문의하십시오.
● JIT 개발의 경우 생성 된 코드를 확인하고 Cache Speculation Side-channels Whitepaper (https://developer.arm.com/support/security-update/download-the-whitepaper)에 설명 된대로 새로운 명령어 시퀀스로 교체하십시오 .
● Variant 1: bounds check bypass (CVE-2017-5753) 대응 방안
- Cache Speculation Side-channels whitepaper에 설명 된 코드 스니펫을 검색
- Compiler support for mitigations(https://developer.arm.com/support/security-update/compiler-support-for-mitigations)에 따라 코드를 재컴파일하고 컴파일러를 업데이트
● Variant 2: branch target injection (CVE-2017-5715)
- 커널 패치 및 Arm Trusted Firmware 패치 적용
https://git.kernel.org/pub/scm/linux/kernel/git/arm64/linux.git/log/?h=kpti
https://github.com/ARM-software/arm-trusted-firmware/wiki/ARM-Trusted-Firmware-Security-Advisory-TFV-6
● Variant 3: rogue data cache load (CVE-2017-5754)
- 커널 패치 및 Arm Trusted Firmware 패치 적용
https://git.kernel.org/pub/scm/linux/kernel/git/arm64/linux.git/log/?h=kpti
https://github.com/ARM-software/arm-trusted-firmware/wiki/ARM-Trusted-Firmware-Security-Advisory-TFV-6

ARM 취약점 대응현황 (https://developer.arm.com/support/security-update)

▶ 영향을받는 코어만 표시되며 다른 모든 ARM 코어는 영향을받지 않습니다 .

Processor	Variant 1	Variant 2	Variant 3	Variant 3a
Cortex-R7	Yes*	Yes*	No	No
Cortex-R8	Yes*	Yes*	No	No
Cortex-A8	Yes (under review)	Yes	No	No
Cortex-A9	Yes	Yes	No	No
Cortex-A15	Yes (under review)	Yes	No	Yes
Cortex-A17	Yes	Yes	No	No
Cortex-A57	Yes	Yes	No	Yes
Cortex-A72	Yes	Yes	No	Yes
Cortex-A73	Yes	Yes	No	No
Cortex-A75	Yes	Yes	Yes	No

* Note for Cortex-R cores: The common usage model for Cortex-R is in non-open environments where applications or processes are strictly controlled and hence not exploitable.

[그림.8] 영향받는 ARM 프로세스 목록 (https://developer.arm.com/support/security-update)

Chrome Project

해당 취약점은 JavaScript 및 WebAssembly 를 지원하는 Chrome 및 기타 브라우저를 비롯하여 외부에서 제공되는 코드를 실행하는 제품 및 서비스에 영향을 미칩니다

또한 Google 제품에 대한 취약점 정보는 다음에서 확인 가능하다.
(https://support.google.com/faqs/answer/7622138)

Chrome을 사용하면 사용자가 사이트 격리라는 옵션 기능을 사용하도록 설정하여 이러한 취약점 악용을 완화 할 수 있습니다. 사이트 격리를 사용하면 Chrome이 별도의 프로세스에서 열려있는 웹 사이트의 콘텐츠를 렌더링 할 때 Speculation Side-channels 공격에 노출 된 데이터가 줄어 듭니다.

Chrome의 자바 스크립트 엔진 인 V8 에는 Chrome 64부터 2018 년 1 월 23 일경에 출시 될 완화 조치가 포함됩니다. 향후 Chrome 버전에는이 완화 등급의 영향을 줄이기위한 추가 완화 및 강화 조치가 포함됩니다. 또한 SharedArrayBuffer 기능은 기본적으로 사용하지 않도록 설정되어 있습니다.

사용자 권고 사항

1. 가능한 SamStime와 HTTPOnly cookie attributes의 렌더러 프로세데스 쿠키 방지 기능을 사용
2. Document.cookie 스크립트 읽기 기능 차단
3. MIME 유형이 올바른지 확인 하고 사용자 별 또는 중요 내용이있는 URL에 대해 nosniff 헤더를 지정
4. 사이트 격리가 설정된 사용자에 대한 Cross-site document 차단 기능을 활용

Chrome Project 취약점 대응게시판 (https://www.chromium.org/Home/chromium-security/ssca)

Intel

Intel 악의적 인 목적으로 사용될 때 설계된대로 작동하는 컴퓨팅 장치에서 중요한 데이터를 부적절하게 수집 할 수있는 소프트웨어 분석 방법을 설명하는 새로운 보안 연구에 대해 알고 있습니다. 인텔은 이러한 익스플로잇이 데이터 손상, 수정 또는 삭제의 가능성이 없다고 생각합니다.

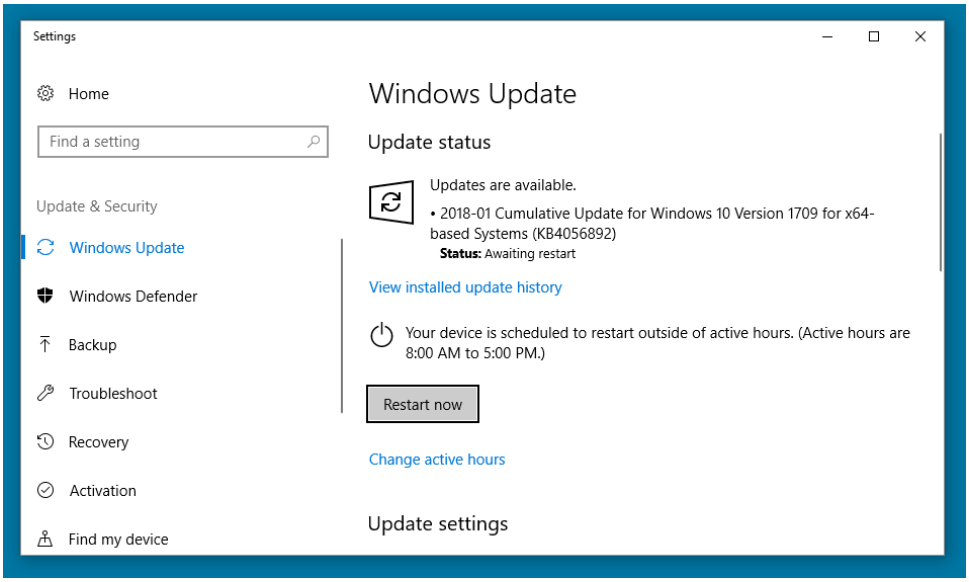
MORE : 인텔이 보안 취약점으로부터 시스템을 보호하기 위해 업데이트했습니다 (2018 년 1 월 4 일)
(https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/)
보안 취약성 및 인텔 제품 (보도 자료 키트)
(https://newsroom.intel.com/press-kits/security-exploits-intel-products/)
새로운 보안 연구 결과 및 인텔 제품 정보
(https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html)

이러한 악용은 "버그"또는 "결함"으로 인해 발생하며 인텔 제품에만 고유 한 최신 보고서는 잘못되었습니다. 현재까지의 분석을 기반으로, 다양한 벤더의 프로세서 및 운영 체제가있는 많은 유형의 컴퓨팅 장치가 이러한 공격에 취약합니다.

Intel 취약점 대응게시판 (https://newsroom.intel.com/news/intel-responds-to-security-research-findings/)

Microsoft

2018 년 1 월 3 일 Microsoft 는 Windows 7 SP1, Windows 8.1, Windows 10 및 다양한 Windows Server 버전에 대한 긴급 업데이트를 릴리스했습니다. 이 업데이트는 Spectre and Meltdown 의 Speculation Side-channels 취약점을 완화하는 데 도움이되지만 완벽하게 보호하려면 컴퓨터에 최신 펌웨어 및 BIOS 업데이트를 설치해야합니다.



[그림.9] Windows Update 화면

Speculation Side-channels 취약점으로부터 보호하기위한 Windows Server Guidance (https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution)
IT 전문가가 Speculation Side-channels 취약점으로부터 보호하는 Windows 클라이언트 지침 (https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in)

Mozilla

모질라는 파이어 폭스의 이전 버전이 이러한 공격을 받기 쉽다는 권고를 발표했다. Mozilla 는 이러한 공격을 완화하기 위해 Firefox 57 부터 Firefox 의 internal timer functions 의 정밀도를 감소 시켰습니다. 따라서 모든 Firefox 사용자는 추가 보호를 위해 Firefox 57 로 업그레이드해야합니다.

Mozilla 취약점 대응게시판 (https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/)

Nvidia

GPU 하드웨어가 보고된 보안 문제에 영향을 받지 않으며 CPU 보안 문제를 완화하기 위해 GPU 드라이버를 업데이트하고 있다고 생각합니다. ARM CPU를 사용하는 SoC의 경우, 영향을받은 사항을 파악하고 적절한 완화 조치를 준비하고 있습니다.

Nvidia 포럼 (https://forums.geforce.com/default/topic/1033210/nvidias-response-to-speculative-side-channels-cve-2017-5753-cve-2017-5715-and- cve-2017-5754 /)

Redhat

Red Hat 제품의 영향을받는 버전을 실행중인 Red Hat 고객은 바로 업데이트 할 것을 강력히 권장합니다. 고객은 해당 업데이트를 즉시 적용해야합니다. 영향을받는 모든 제품은 CVE-2017-5753 (변형 1) 및 CVE-2017-5754 (변형 3) 을 완화하기위한 수정을 적용해야합니다/ CVE-2017-5715 (변형 2)는 로컬 및 가상화 게스트 경계를 통해 악용 될 수 있습니다

Nvidia 포럼 (https://forums.geforce.com/default/topic/1033210/nvidias-response-to-speculative-side-channels-cve-2017-5753-cve-2017-5715-and- cve-2017-5754 /)

Updates for Affected Products

Product	Applicable to Variant	Package	Advisory/Update
Red Hat Enterprise Linux 7	1,2,3	kernel	RHSA-2018:0007
Red Hat Enterprise Linux 7	1,2,3	kernel-rt	RHSA-2018:0016
Red Hat Enterprise Linux 7	2	libvirt	RHSA-2018:0029
Red Hat Enterprise Linux 7	2	qemu-kvm	RHSA-2018:0023
Red Hat Enterprise Linux 7	2	dracut	RHBA-2018:0042
Red Hat Enterprise Linux 7.3 Extended Update Support**	1,2,3	kernel	RHSA-2018:0009
Red Hat Enterprise Linux 7.3 Extended Update Support**	2	libvirt	RHSA-2018:0031
Red Hat Enterprise Linux 7.3 Extended Update Support**	2	qemu-kvm	RHSA-2018:0027
Red Hat Enterprise Linux 7.3 Extended Update Support**	2	dracut	RHBA-2018:0043
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	1,2,3	kernel	RHSA-2018:0010
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	2	libvirt	RHSA-2018:0032
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	2	qemu-kvm	RHSA-2018:0026
Red Hat Enterprise Linux 7.2 Advanced Update Support***,****	2	dracut	pending
Red Hat Enterprise Linux 6	1,2,3	kernel	RHSA-2018:0008
Red Hat Enterprise Linux 6	2	libvirt	RHSA-2018:0030
Red Hat Enterprise Linux 6	2	qemu-kvm	RHSA-2018:0026
Red Hat Enterprise Linux 6.7 Extended Update Support**	1,2,3	kernel	RHSA-2018:0011
Red Hat Enterprise Linux 6.7 Extended Update Support**	2	libvirt	pending
Red Hat Enterprise Linux 6.7 Extended Update Support**	2	qemu-kvm	pending
Red Hat Enterprise Linux 6.6 Advanced Update Support***,****	1,2,3	kernel	RHSA-2018:0017
Red Hat Enterprise Linux 6.6 Advanced Update Support***,****	2	libvirt	pending
Red Hat Enterprise Linux 6.6 Advanced Update Support***,****	2	qemu-kvm	pending
Red Hat Enterprise Linux 6.5 Advanced Update Support***	1,2,3	kernel	RHSA-2018:0022
Red Hat Enterprise Linux 6.5 Advanced Update Support***	2	libvirt	pending
Red Hat Enterprise Linux 6.5 Advanced Update Support***	2	qemu-kvm	pending
Red Hat Enterprise Linux 6.4 Advanced Update Support***	1,2,3	kernel	RHSA-2018:0018
Red Hat Enterprise Linux 6.4 Advanced Update Support***	2	libvirt	pending
Red Hat Enterprise Linux 6.4 Advanced Update Support***	2	qemu-kvm	pending
Red Hat Enterprise Linux 6.2 Advanced Update Support***	1,2,3	kernel	RHSA-2018:0020
Red Hat Enterprise Linux 6.2 Advanced Update Support***	2	libvirt	pending

[그림.10] RedHat 영향받는 버전 업데이트 정보

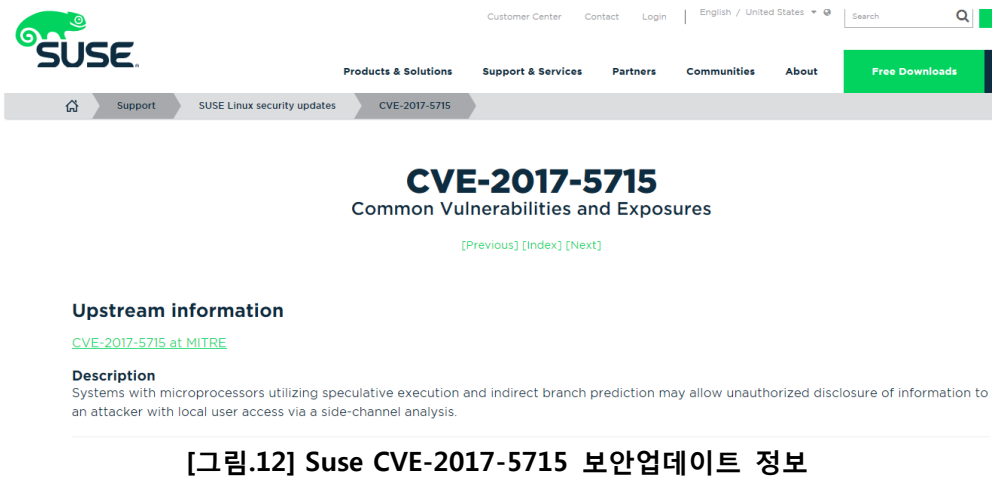
(https://access.redhat.com/security/vulnerabilities/speculativeexecution?sc_cid=701f2000000tsLNAAY&)

Suse

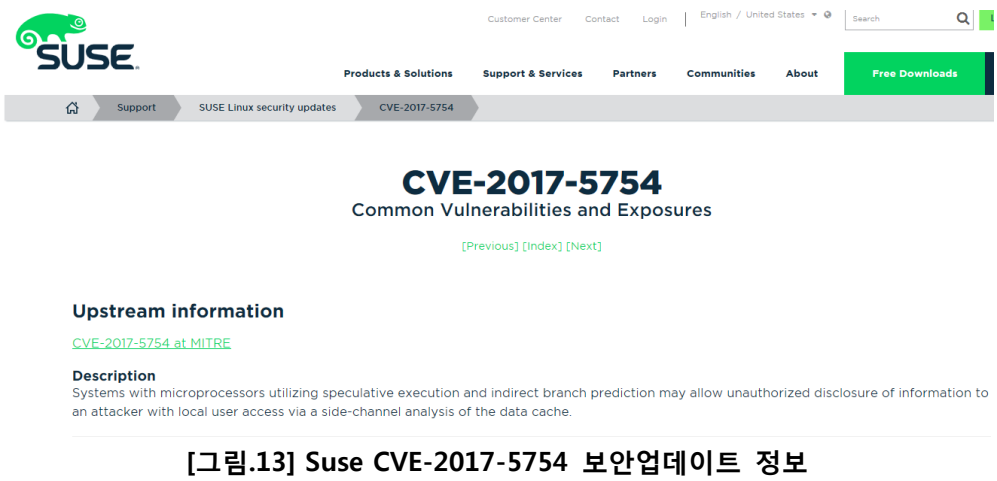
SUSE 엔지니어들은 협력 업체 및 Linux 커뮤니티와 업스트림 Linux 커널 패치를 통해 협력 해 왔습니다. 그 협업의 결과로, 우리는 이제 최신 SUSE Linux Enterprise (SLE) 버전에 대한 패치를 릴리스 할 수있게되었습니다. 다른 SLE 버전 및 환경을위한 추가 패치가 곧 제공 될 것입니다.

취약점 보안 업데이트 페이지(https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/)

[그림.11] Suse CVE-2017-5753 보안업데이트 정보



[그림.12] Suse CVE-2017-5715 보안업데이트 정보



[그림.13] Suse CVE-2017-5754 보안업데이트 정보

VMware

취약점 관련제품
- VMware vSphere ESXi (ESXi)
- VMware Workstation Pro / Player (워크 스테이션)
- VMware Fusion Pro / Fusion (퓨전)

CPU 데이터 캐시 타이밍은 잘못 추측 된 CPU 실행에서 정보를 누출하여 임의의 가상 메모리가 다양한 컨텍스트의 로컬 보안 경계를 통해 (최악의 경우) 읽기 취약점으로 이어질 수 있습니다. ESXi, Workstation 및 Fusion은이 취약점으로 인한 Bounds Check Bypass 및 Branch Target Injection 문제에 취약합니다.

취약점으로 인해 가상 컴퓨터의 동일한 호스트에서 실행중인 게스트 OS의 정보 유출을 허용 할 수 있습니다.

VMware Product	Product Version	Running on	Severity	Replace with/ Apply Patch	Mitigation/ Workaround
ESXi	6.5	Any	Important	ESXi650-201712101-SG	None
ESXi	6.0	Any	Important	ESXi600-201711101-SG	None
ESXi	5.5	Any	Important	ESXi550-201709101-SG*	None
Workstation	14.x	Any	N/A	Not affected	N/A
Workstation	12.x	Any	Important	12.5.8	None
Fusion	10.x	OS X	N/A	Not affected	N/A
Fusion	8.x	OS X	Important	8.5.9	None

* This patch has remediation against CVE-2017-5715 but not against CVE-2017-5753.

[그림.14] VM 제품 보안 업데이트 정보 (https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html)

Sniper 제품군 대응 방안

Sniper 제품군은 1 월 12 일(금) 정규 릴리즈 'Processor Spectre Memory Info Disclosure' 예정되 있습니다.

Snort 임시 패턴

```
alert TCP any 80 -> any any (msg:"Processor Spectre Memory Info Disclosure"; flow:to_client;
content:"TABLE1_STRIDE|29 7C 30|"; content:"TABLE1_BYTES-1|29 29 7C 30|"; distance:0; priority:1; sid:0;)
```

▶ 정오탐 테스트가 완료되지 않은 패턴으로 각 사이트에서는 패턴 적용시 참고하시기 바랍니다.

㈜윈스는

윈스는 향후 지속적인 성장이 예상되는 정보보호산업에서 최고의 기술력과 시장지배력 및 효율적인 경영시스템을 갖춘 보안솔루션 기업을 목표로, 첫째 네트워크 핵심 기술력 기반의 통합 해킹공격 탐지/웜바이러스 탐지기술을 중심축으로 관련 아이템을 개발하는 네트워크 정보보호 전문기업을 지향합니다. 둘째 전략적 제휴를 통한 수평적, 수직적 사업네트워크를 구축하여 세계적인 네트워크 기술 보유기업으로서 정보보호의 선두를 지향합니다. 셋째 '고객만족'을 기본원칙으로 한 완벽한 기술지원서비스로 고객으로 하여금 '믿음직한 기업'의 이미지 구축, 신뢰를 바탕으로 한 우량기술기업을 지향합니다.

㈜윈스

경기도 성남시 분당구 삼평동 633 판교세븐벤처밸리 1동 4층

TEL : 031)622-8600

E-Mail : cert@wins21.co.kr

Visit Our Blog

http://wins21.co.kr/blog/blog.html

Visit Our Homepage

http://securecast.co.kr