제목	GigaByte Bios Update Test	
문서 작성일 및 작성자	최초 작성일	2018년 1월 22일
	최종 수정일	2018년 1월 22일
	테스터	인프라 운영팀
BMT목적	Bios 업데이트를 통한 멜트다운 버그및 스펙터 버그 패치 가능성 확인	
TEST 시스템	CPU : Intel E3-1230 V6 M/B : GigaByte MX31 RAM : SAMSUNG DDR4 16G E/U HDD : 128G SSD CASE : case less POWER : 500Wat OS : CentOS 6.X 64Bit	
BMT 결과	Bios Update는 멜트다운 버그와 스펙터 버그를 해결 불가능	
목차	1. Test 진행 방법 소개 2. 버그 해결 여부. 3. 퍼포먼스 비교. 4. 결론	

1. Test 진행 과정은 다음과 같다.

1)바이오스 업데이트 후 버그 해결 확인

2)non 패치 상황에서 시스템의 퍼포먼스를 확인.

3)추가로 OS 패치(멜트다운 패치) 진행 후 시스템 퍼포먼스 확인.

2. Bios Update를 통한 버그 해결 여부.

BIOS(+2)

Version	Size	Date	Download	Description
R05	14.83 MB	2018/01/16	Asia China America Europe	Fixed new kernel boot legacy mode USB can't work
R07	14.22 MB	2018/01/16	Asia China America Europe	Updated Microcode for Security problem

1월 16일자 보안 관련 마이크로 코드 업데이트 펌웨어.

바이오스 패치 전 시스템 취약성 확인.

```
Spectre and Meltdown mitigation detection tool v0.31

Checking for vulnerabilities against running kernel Linux 2.6.32-696.el6.x86_64 #1 SMP Tue Mar 21 19:29:05 UTC 2017 x86_64
CPU is Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz

CVE-2017-5753 [bounds check bypass] aka 'Spectre Variant 1'
* Checking count of LFENCE opcodes in kernel: NO
> STATUS: VULNERABLE (only 27 opcodes found, should be >= 70, heuristic to be improved when official patches become available)

CVE-2017-5715 [branch target injection] aka 'Spectre Variant 2'
* Mitigation 1
*   Hardware (CPU microcode) support for mitigation
*     The SPEC_CTRL MSR is available: NO
*     The SPEC_CTRL CPUID feature bit is set: NO
*   Kernel support for IBRS: NO
*   IBRS enabled for Kernel space: NO
*   IBRS enabled for User space: NO
* Mitigation 2
*   Kernel compiled with retpoline option: NO
*   Kernel compiled with a retpoline-aware compiler: NO
> STATUS: VULNERABLE (IBRS hardware + kernel support OR kernel with retpoline are needed to mitigate the vulnerability)

CVE-2017-5754 [rogue data cache load] aka 'Meltdown' aka 'Variant 3'
* Kernel supports Page Table Isolation (PTI): NO
```

```
* PTI enabled and active: NO
* Checking if we're running under Xen PV (64 bits): NO
> STATUS: VULNERABLE (PTI is needed to mitigate the vulnerability)

A false sense of security is worse than no security at all, see –disclaimer
```

바이오스 패치 후 취약성 확인.

```
Spectre and Meltdown mitigation detection tool v0.32

Checking for vulnerabilities against running kernel Linux 2.6.32-696.el6.x86_64 #1 SMP Tue Mar 21 19:29:05 UTC 2017 x86_64
CPU is  Intel(R) Xeon(R) CPU E3-1230 v6 @ 3.50GHz

CVE-2017-5753 [bounds check bypass] aka 'Spectre Variant 1'
* Checking count of LFENCE opcodes in kernel: NO
> STATUS: VULNERABLE (only 27 opcodes found, should be >= 70, heuristic to be improved when official patches become available)

CVE-2017-5715 [branch target injection] aka 'Spectre Variant 2'
* Mitigation 1
*   Hardware (CPU microcode) support for mitigation
*     The SPEC_CTRL MSR is available: YES
*     The SPEC_CTRL CPUID feature bit is set: NO
*   Kernel support for IBRS: NO
*   IBRS enabled for Kernel space: NO
*   IBRS enabled for User space: NO
* Mitigation 2
*   Kernel compiled with retpoline option: NO
*   Kernel compiled with a retpoline-aware compiler: NO
> STATUS: VULNERABLE (IBRS hardware + kernel support OR kernel with retpoline are needed to mitigate the vulnerability)

CVE-2017-5754 [rogue data cache load] aka 'Meltdown' aka 'Variant 3'
* Kernel supports Page Table Isolation (PTI): NO
* PTI enabled and active: NO
* Checking if we're running under Xen PV (64 bits): NO
> STATUS: VULNERABLE (PTI is needed to mitigate the vulnerability)

A false sense of security is worse than no security at all, see –disclaimer
```

위 결과처럼 바이오스 패치를 하여도 멜트다운, 스펙터 모두 취약한 상태로 표시됨.
단 스펙터 2 버그 중 The SPEC_CTRL MSR is available: YES. 스펙터 버그를 해결하기 위함으로,
OS에서의 커널 업데이트와 바이오스의 마이크로코드 업데이트가 모두 갖춰져야 패치가 되기 때문.

다시한번 정리하면.
(1)바이오스 업데이트만으로는 멜트다운, 스펙터 버그 모두 해결할 수 없음.
(2)멜트다운 버그는 OS 업데이트만으로 해결 가능.
(3)스펙터버그는 두개의 취약점이 존재하며 그중 하나는 바이오스의 업데이트가 필수적.
(4)즉 멜트다운 버그와 스펙터버그 모두 해결하기 위해선 바이오스 업데이트와 OS 패치 모두 필요함.

3. 패치 후 퍼포먼스 하락 확인.

1) UnixBench

시스템 전반에 걸친 종합 성능 테스트(높을수록 좋음)

패치 종류	Non	OS	Bios & OS
점수	7346.9	4632.1	4644.8

2) C-ray

CPU의 성능을 파악하는 툴(낮을수록 좋음)

패치 종류	Non	OS	Bios & OS
점수	37.62	37.62	37.66

3) IOZONE

디스크 입출력 성능을 테스트(높을수록 좋음)

패치 종류	Non	OS	Bios & OS
랜덤 읽기	314685	321801	312842
램덤 쓰기	147065	145379	137660

4)퍼포먼스 결과.

첫번째 테스트였던 UnixBench에서는 대략 36%의 성능 하락을 보임.
하지만 2개의 단독테스트에서는 성능 하락은 보이지 않음.
멜트다운에 패치에 추가로 BIOS업뎃을 통한 성능하락은 아직까지 발견되지 않음.

4. 종합 분석 및 결론.

퍼포먼스 테스트 부분은 Mysql설치후 실제 걸리는 시간 계측등, 더욱 심도 깊은 테스트가 필요함.
실제 사용시에 요구되는 테스트 필요. AMD와 Intel간의 퍼포먼스 차이 테스트할때 계측할 예정.
GigaByte 보드의 경우 Bios 업데이트 후에 성능 하락 없음.
하지만 다른 제작사도 그렇다는 보장은 없음. Asrock에도 마이크로코드 바이오스 업데이트를 내놓을 예정.

바이오스 업데이트를 통한 멜트다운 버그 해결부분은 불가능하며 스펙터 버그를 위한 업데이트.