

www.datastoragecorp.com

Security Briefing.... Meltdown / Spectre Exploits on IBM i





Meltdown and Spectre Exploits What are they?



- Meltdown and Spectre are different variants of the same underlying vulnerability
- They make use of 'Speculative Execution' to perform side-channel information disclosure attacks
- They affect nearly every processor made in the last 20 years (including IBM Power)

Premier Cloud Provider for IBM i and AIX



Meltdown and Spectre Exploits What do they exploit?



• The vulnerabilities work by exploiting:

Speculative Execution

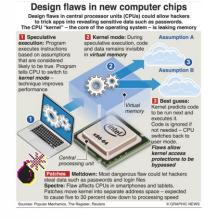
 Speculative Execution allows a CPU to process multiple branches of a logic statement at the same time before the answer to the initial logic is known.

----AND----

CPU Caching

 Caching speeds up RAM using CPU cache which gets filled with data that the CPU will need soon or often

Premier Cloud Provider for IBM i and AIX





Meltdown and Spectre Exploits Who is Affected?



Who is Aff	Who is Affected			
👰 Meltdown Only				
	(intel)			
.∰∕ Spectre Only				
	IBM arm			
L ALCONTRACTOR	arm	(intel)		
	100	VH01		
Premier Cloud Provid	ler for IBM i	and AIX	-Data	





Meltdown

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies both to personal computers as well as cloud infrastructure. Luckily, there are software patches against Meltdown.

Spectre

Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre

Spectre is harder to exploit than Meltdown, but it is also harder to mitigate. However, it is possible to prevent specific known exploits based on Spectre through software patches.

Premier Cloud Provider for IBM i and AIX



Meltdown and Spectre Exploits What to do for IBM i ?

- System updates
 - PTFs are available for IBM i 7.1, 7.2 and 7.3
 - Power System Firmware must also be applied

* *Important note:* IBM recommends that all users running unsupported versions of affected products upgrade to supported and fixed version of affected products.

Follow Security Best Practices for IBM i

Premier Cloud Provider for IBM i and AIX



Meltdown and Spectre Exploits More Information

Links:

- IBM **PSIRT** Blog (Product Security Incident Response)
 - <u>https://www.ibm.com/blogs/psirt/</u>
 - <u>https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/</u>

- IBM Support Bulletin: IBM i

- http://www-01.ibm.com/support/docview.wss?uid=nas8N1022433
- IBM Security Bulletins
 - https://www.ibm.com/security/secure-engineering/bulletins.html

Premier Cloud Provider for IBM i and AIX



Meltdown and Spectre Exploits https://xkcd.com/1938/ THE MELTDOWN AND SPECTRE. EXPLOITS USE "SPECULATIVE EXECUTION?" WHAT'S THAT? THE PHANTOM TROLLEY ISN'T SUPPOSED TO TOUCH ANYONE. **Thank You!** BUT IT TURNS OUT YOU CAN STILL USE IT TO DO STUFF. YOU KNOW THE TROUFY PROBLEM? LIEL You know the trouley problem? Uell, for a while nou, CPUs have basically been sending trouleys down both Paths, quantum-stve, while awarting Your Choice. Then the Unneeded AND IT CAN DRIVE ROUGH WALLS PHANTOM" TROLLEY DISAPPEARS. JHAT'S THAT? THAT SOUNDS BAD. SO YOU'RE SAYING IF YOU TOGGLE A ROW OF MEMORY CELLS ON AND OFF REALLY FAST, YOU CAN USE ELECTRICAL INTERFERENCE THE CLOUD IS FULL OF HONESTLY, I'VE BEEN PHANTOM TROLLEYS ASSUMING WE WERE ARMED WITH HAMMERS. DOOMED EVER SINCE TO FLIP NEARBY BITS AND-I LEARNED ABOUT ...YES, THAT IS DO WE JUST SUCK AT...COMPUTERS? EXACTLY RIGHT ROUHAMMER. OKAY TULUH. YUP ESPECIALLY SHARED ONES. INSTALL UPDATES? (Sj GOOD IDEA. SPECTRE **MELTDOWN**

Premier Cloud Provider for IBM i and AIX www.datastoragecorp.com

