Tonga National Computer Emergency Response Team

“Meltdown and Spectre” CPU Flaws

Dear Constituents,

Two vulnerabilities dubbed as **Meltdown** and **Spectre** have been identified and they affect all critical vulnerabilities in modern processors (CPU), a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This includes your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

How they work

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers.

- **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.
- **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.

Impact

These vulnerabilities can allow an attacker to execute code with user privileges. The Meltdown attack allows reading of kernel memory from user space. Resulting in privilege escalation, disclosure of sensitive information. The Spectre attack can allow inter-process or intra-process data leaks.

How to protect yourself

- Ensure that all software on you device is up-to-date with the latest updates
- Keep your browser such as Firefox, Chrome, Opera, Safari, Internet Explorer be updated.

- Please ***NOTE***: Different OS vendors such as Microsoft, Linux and Apple have updated patches. Applying the update patches will remove shared kernel mapping which prevents the ability to predict values in protected memory. Unfortunately, by removing this feature, a lot of processing efficiency is removed as well. This will result in some performance decrease for those systems. What that decrease is will depend on how heavily software relies on this memory access, but current estimates suggest anywhere from a ***5%-30% decrease*** in overall software performance.

Reference

https://winaero.com/blog/microsoft-rolling-emergency-fix-meltdown-spectre-flaws/
https://meltdownattack.com/
https://docs.google.com/spreadsheets/d/184wcDt9I9TUNFFbsAVLpzAtckQxYiuirADzf3cL42FQ/edit#gid=0
https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-updates-to-fix-meltdown-and-spectre-cpu-flaws/
https://spectreattack.com/
https://www.cert.govt.nz//it-specialists/advisories/advisory/meltdown-and-spectre-cpu-vulnerabilities?utm_medium=email&utm_campaign=Meltdown%20and%20Spectre%20CPU%20vulnerabilities_275_1515442549&utm_content=Meltdown%20and%20Spectre%20CPU%20vulnerabilities_275_1515442549+CID_da6cb1927e8a8ae8f668abaf7e22c3b1&utm_source=CM%20emails&utm_term=Read%20more
https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html
https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=926

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.to
web: www.cert.to