INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

# Major security flaw discovered in processors

*You are receiving this email because you are subscribed to UIT's public email list.*

*Note: This message is also being sent to NotifyIT security subscribers via SMS and email.*

**Summary:**
A series of security exploits in chips from Intel and AMD have been discovered that, if exploited, could allow criminals to access data stored in the memory on your device(s). The flaws, known as Spectre and Meltdown, potentially allow access to passwords, encryption keys, or sensitive information open in applications. Intel does not believe these exploits have the potential to corrupt, modify, or delete data.

**Impact:**
The University's Information Security Office is aware of the issue and is closely monitoring developments. Patches to mitigate the risks posed by the exploits are already available from some vendors, and others will release patches soon.

**Recommendations:**
Users should ensure their devices are up to date with currently-available patches, and apply Spectre and Meltdown updates to devices' software as soon as they are available.

**More information:**

- https://meltdownattack.com
- http://bit.ly/meltdown-and-spectre
- http://bit.ly/intel-chip-flaw

If you have questions or need assistance, please contact your respective help desk: UIT Help Desk at 801-581-4000, option 1; ITS Service Desk at 801-587-6000.

***Node 4 story idea? Email us: stratcomm@it.utah.edu***

***it.utah.edu***

**NotifyIT** | **Follow us on Twitter** | **IT Services Status** | **IT Service Portal**