WHAT IS THE CONCERN?
A set of security vulnerabilities that affect modern computer processors has been discovered. These vulnerabilities, labeled Spectre and Meltdown, could allow an attacker access to sensitive information. Unlike previous vulnerabilities, these are found in the CPU architecture rather than software, so patching may not resolve the vulnerabilities in all scenarios.

WHO IS AFFECTED?
Most systems (computers, laptops, servers, and mobile devices) that contain CPUs—especially Intel CPUs—are affected, but the risk is not limited to Intel.

WHAT ACTION DO I NEED TO TAKE?
Many Operating System (OS) vendors have provided updates for the vulnerabilities.

- Make sure your system is up to date. Install software updates for Microsoft, Apple, Google, Red Hat, etc.
- Install hardware updates that are available for systems by checking manufacturers’ websites – Dell, HP, Lenovo, Apple, etc.
- View this chart with links to advisories and patches published in response to the vulnerabilities.

ADDITIONAL RESOURCES

- CERT/CC's Vulnerability Note VU #584653
- Google Project Zero Blog
- Research Papers

If you need assistance please call 325-HELP (4357) during normal business hours, or visit needhelp.ou.edu at any time.