

Vendors Rush to Patch Meltdown and Spectre Vulnerabilities

By Allan Liska

Appendix A - References

Links to the Intel security advisories:

<https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr>

<https://01.org/security/advisories/intel-oss-10002>

<https://01.org/security/advisories/intel-oss-10003>

Links to the Google security advisory:

<https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>

<https://blog.google/topics/google-cloud/what-google-cloud-g-suite-and-chrome-customers-need-know-about-industry-wide-cpu-vulnerability/>

Link to the Amazon security bulletin:

<https://aws.amazon.com/security/security-bulletins/AWS-2018-013/>

Links to multiple other vendors' security advisories:

<https://chrisam.net/2018/01/04/speculative-execution-side-channel-vulnerabilities-vendor-published-info/>

Microsoft Windows Update:

<https://support.microsoft.com/en-us/help/4072699/important-information-regarding-the-windows-security-updates-released>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002>

CERT Vulnerability Report:

<https://www.kb.cert.org/vuls/id/584653>

Recorded Future arms security teams with threat intelligence powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context that's delivered in real time and packaged for human analysis or instant integration with existing security technology.