THE
NATIONAL LAW REVIEW

Vulnerabilities to Most Computer Processors Revealed

Tuesday, June 26, 2018

In the first week of the New Year, we learned that most computer processor chips sold over the past 10 years are vulnerable to side-channel attacks. These vulnerabilities, dubbed Spectre and Meltdown, could grant a hacker access to sensitive information, such as passwords and other personal information. Unlike software vulnerabilities seen in the likes of the WannaCry attacks, according to the US Computer Emergency Readiness Team (US-CERT), Spectre and Meltdown may require more than patches for protection since the vulnerability is in the chip itself. In the short term, however, installing patches or updates may still be the best bet. Chip manufactures are working to push out updates. US-CERT warns that the updates may diminish performance by up to 30% and recommends close performance monitoring. See the US-CERT page for information on patch availability and recommendations. In addition to patching, companies should monitor systems closely for suspicious activity and data leaks and should immediately implement the company incident response plan if there are any signs or indications that data has been improperly accesses or removed.

Article By Murtha Cullina
Dena M. Castricone
Privacy and Cybersecurity Perspectives

Communications, Media & Internet
All Federal

Source URL: https://www.natlawreview.com/article/vulnerabilities-to-most-computer-processors-revealed