

Congress of the United States
Washington, DC 20515

July 17, 2018

Roberta Stempfley
Director
The Software Engineering Institute
CERT Coordination Center
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Dear Ms. Stempfley:

Following the public disclosure of the Spectre and Meltdown chip vulnerabilities on January 3, 2018, the Committee on Energy and Commerce in the U.S. House of Representatives and the Committee on Commerce, Science, and Transportation in the U.S. Senate sent letters to affected companies seeking information about their coordinated vulnerability disclosure (CVD) practices.¹ The Committees' original concerns centered on different stakeholders' equities in CVD processes, as well as the timing, coordination, effectiveness, and impact of the processes. The responses provided by the recipients raise questions about the coordination of the CVD process and also suggest the lack of precision in describing the availability or implementation of patches could give both companies and users a false sense of security.

Spectre and Meltdown are serious cybersecurity vulnerabilities affecting nearly all modern computing systems. Originally discovered in June 2017 by researchers at Google's Project Zero (GPZ), the vulnerabilities were tested, verified, and addressed by a core group of companies. These companies imposed an information embargo on details relating to the vulnerabilities, and scheduled a public disclosure date of January 9, 2018. However, for various reasons, information about the vulnerabilities began to appear publicly prior to that date, and the companies decided to move up their public disclosure to January 3, 2018. The Committees' original letters provide additional details on the initial disclosure.²

¹ Letters from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. on Energy and Commerce, to Apple, Inc., Amazon, Advanced Micro Devices, Inc., ARM Holdings, PLC, Google, Inc., Intel Corp., and Microsoft Corp. (Jan. 24, 2018); Letters from the Hon. John Thune and Hon. Bill Nelson, Sen. Comm. on Commerce, Science, and Transportation, to Advanced Micro Devices, Inc., Amazon.com, Inc., Apple Inc., ARM Holdings PLC, Cisco Systems, Inc., Google LLC, Huawei Technologies, Co., Ltd., Intel Corp., International Business Machines Corp., Lenovo Group Limited, Microsoft Corp., and NVIDIA Corp. (Feb. 15, 2018).

² *Id.*

In May, Intel confirmed the existence of Variant 4 and Variant 3a, derivatives of the vulnerabilities previously disclosed by GPZ in January 2018.³ It also provided information about the new vulnerabilities, updates on Spectre and Meltdown, and advice on how to protect computer systems and information. These new developments underscore the need to continually improve CVD processes.

Vulnerabilities as pervasive and serious as Spectre and Meltdown can necessitate massively complex, multi-party CVDs, and the core group of companies that addressed these vulnerabilities deserve credit for an overall effective and successful mitigation effort. However, it is important in the aftermath of such incidents to examine the processes used to identify potential improvements and lessons learned. The Committees have analyzed the responses from companies in the core group involved in the Spectre and Meltdown CVD, and believe there are two major lessons learned: the adequacy of coordination and the misapplication of such terms as “in place” and “available” when used to describe the status of vulnerability patches.

In their responses to the Committees’ letters, many of the companies explained that it is industry best practice to embargo vulnerability information amongst the smallest possible group of stakeholders during CVDs to prevent “bad actors” from learning of the vulnerability or vulnerabilities before they have been corrected. Many of the companies further advised that they followed or otherwise cited the CVD protocol or guidance provided by the CERT Coordination Center (CERT/CC). In addition, many respondents further argued that it is critical to do so to ensure that patches are “in place,” “delivered,” or “implemented” prior to widespread public disclosure.⁴ As a company or user is not protected from a given vulnerability until an appropriate patch is “in place,” “delivered,” or “implemented,” we agree that sound CVD strategies would seek to limit disclosure of vulnerability information before stakeholders are able to apply patches. Such a practice allows for the best protection of the end user—typically, consumers.

However, based on the responses to our letters and information provided during company briefings, questions remain regarding: (1) whether the CVD process was adequately coordinated to ensure that companies, particularly those providing critical infrastructure, had enough time to test and implement patches prior to public disclosure of the vulnerabilities and that the U.S. government received timely notice of the CVD process; and (2) whether companies used precise terminology in describing the *availability*, not *application*, of patches. Companies outside the core group needed time to test and successfully implement patches, and the availability of a patch and the application of a patch are not the same. The fact that a patch or other mitigation is “available” simply means that it exists and is ready for a company or individual to use. But when a patch or other mitigation is described as “in place,” “delivered,” or “implemented,” the distinction implies that companies and individuals have retrieved that patch and actually applied it to their systems.

³ “Side Channel Methods – Analysis, News and Updates, Facts about Security Research and Intel® Products, May 21, 2018, <https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html>.

⁴ Company responses to letters from the Hon. Greg Walden, Hon. Tim Murphy, Hon. Marsha Blackburn, and Hon. Robert E. Latta, H. Comm. On Energy and Commerce, to Apple, Amazon, AMD, Arm, Google, Intel, and Microsoft (January 24, 2018) available at <https://energycommerce.house.gov/news/letter/letter-tech-companies-meltdown-spectre-vulnerabilities/>.

While security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until early January of 2018. Although all the companies that responded to the Committees' letters advised that they learned about the vulnerabilities through the CVD process prior to January 2018, only one company reported that it informed the U.S. Computer Emergency Readiness Team ("US-CERT") prior to January 2018 --- and it did so in December 2017. Had US-CERT or another federal agency received earlier notice of the CVD process, perhaps it could have helped to coordinate the process more effectively. Indeed, it appears that companies with ties to the Chinese government received notice of the CVD process before US-CERT did. This raises questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities, and as to whether companies providing critical infrastructure had enough time to test and apply patches *before* public disclosure of the vulnerabilities.

In addition to possibly inadequate coordination and untimely notice to US-CERT, the assertion from many of the companies' responses that the companies' release of patches— meaning, their making "available" of patches throughout the first week of January 2018— fully addressed the risk to their users also raises concerns. While this may be true for a limited group of companies like cloud or other "software-as-a-service" providers, which control not only the availability but the application of patches, it is not true for the majority of companies. For those companies, their users are not protected from a given vulnerability until the users take action themselves to apply the patch.

The length of time between when a company makes a patch available and when their users apply the patch to their systems can be as short as a few days. However, companies in critical infrastructure and similar sectors must exhaustively test patches before application to ensure that the patches will not result in adverse secondary consequences. This can lead to a lag time of weeks or months before a patch is applied. In both cases, the lag time between when a patch is "available" and "applied" can provide opportunities for "bad actors" to exploit the vulnerability. Failure to adequately coordinate the CVD process and provide timely notice to companies that need to test patches extensively before applying them can significantly increase the risks associated with the vulnerabilities.

The Committees acknowledge and appreciate that companies making patches available for their products typically have little to no control over the patching practices of their users. We do not point out the language inconsistency to suggest that respondents inappropriately managed the Spectre and Meltdown CVD. Rather, we do so in recognition of the fact that the Internet and the broader connected technology ecosystem now include not only more traditional consumer-based products like smartphones and personal computers, but critical infrastructure technologies like smart grid components and medical devices. As such, the potential consequences of vulnerability exploitation have increased in scope and severity.

We are further concerned that the misapplication of such terms as "in place" regarding patch availability during CVDs may inadvertently increase the likelihood of vulnerability exploitation by providing a false sense of security. It may, for example, lead companies to make CVD timeline and information dissemination decisions based on an assumption that their users will be protected as soon as, or shortly, after the disclosure has been made public and the patch

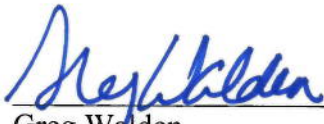
has been released, when in fact those users are vulnerable and will remain so until they can properly test the patches and apply them to their systems.

As the Director of CERT/CC, which developed and now maintains the CERT Guide to Vulnerability Disclosure ("Guide"), you and your organization are uniquely positioned to analyze these concerns and determine if and how CVD policies and procedures should be updated to address them. As noted above, many of the respondents, in fact, cited the Guide as one of the authoritative "best practice" documents on which they relied throughout the Spectre and Meltdown CVD, strongly suggesting that improvements to the Guide would result in widespread dissemination of those improvements in future CVDs.

CVD remains a complex and constantly evolving concept, and as should be expected from one of this size and scale, the Spectre and Meltdown CVD showed that additional improvements can and should be made. The Committees ask that you and your organization consider the issues discussed in this letter and update your policies and procedures to better address them. We further request that you advise us in writing of your plans, if any, to update your policies and procedures, including a timeline for such updates and a description of how they will be communicated to relevant stakeholders.

Thank you for your prompt attention to this letter. If you have any questions, please contact Jessica Wilkerson of the Energy and Commerce Committee at (202) 225-2927, or Cherilyn Pascoe of the Senate Commerce Committee at 202-224-1251.

Sincerely,



Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives



John Thune
Chairman
Committee on Commerce, Science,
& Transportation
U.S. Senate