

July 26, 2018

The Honorable Greg Walden
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable John Thune
Chairman
Committee on Commerce, Science & Transportation
U.S. Senate
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Representative Walden and Senator Thune:

Thank you for the opportunity to respond to your letter dated July 17, 2018, and the concerns of your respective committees.

As noted in your letter, multiparty coordinated vulnerability disclosure (CVD) remains a complicated and unsolved (or unsatisfactorily solved) problem. Hardware-related vulnerabilities like Meltdown and Spectre and the proliferation of connected products and services highlight stress points in multiparty CVD including patch deployment, adequate coordination in advance of public disclosure, and supply chain complexity. Although the CERT Coordination Center (CERT/CC) was not involved in the CVD process for Meltdown and Spectre prior to the public announcement, we appreciate both committees' interest in improving CVD and welcome the opportunity to contribute. In our response, we describe our plans to improve guidance for multiparty CVD and comment on some of the issues raised in your letter.

Before we proceed, we want to emphasize that cybersecurity vulnerabilities are frequently a symptom of development practices that do not adequately consider security, including increasingly complex and connected supply chains.¹ There is a strategic value in improving software engineering practices² in order to reduce the magnitude and widespread deployment of vulnerable systems. Even with the best practice, however, vulnerable systems will exist, so CVD processes are still necessary,

¹ <https://www.ntia.doc.gov/blog/2018/ntia-launches-initiative-improve-software-component-transparency>

² For example: modeling threats in the design phase and following them through to implementation and testing; adopting secure coding practices; focusing attention on finding security bugs in pre-release software through the use of fuzz testing and targeted bug bounties.

and the efforts to optimize the CVD process to react to vulnerabilities in deployed systems remain valuable.

Updating CVD Guidance

We agree there is need to update and clarify guidance around CVD processes. The direct request of the committees is for the CERT/CC to “...consider the issues...” and “...update [our] policies and procedures, including a timeline for such updates and a description of how they will be communicated to relevant stakeholders.”

As the authors and publishers of the *CERT Guide to Coordinated Vulnerability Disclosure*,³ we plan to review the *Guide*, solicit feedback, and publish a revision in early 2019. Additionally, we regularly participate in working groups and standards organizations—including the Forum of Incident Response and Security Teams (FIRST) and International Organization for Standardization (ISO)—that also produce CVD guidance. These efforts operate with their own development rules and schedules, and although we (appropriately) do not control their output or timeframes, we intend to promote any proposed CVD improvements in these venues as well. We will also consider changes to our own CVD processes, particularly regarding more collaborative communication mechanisms.

Throughout our efforts to improve CVD processes, we will discuss changes with a number of stakeholder groups including vendors, researchers, coordinators, governments (including critical infrastructure protection and public safety organizations), and users. For example, we may publish blog posts, host meetings, and give presentations as means to solicit stakeholder and community feedback on the changes we will be making to the *Guide*.

In consideration of planned updates to CVD guidance, we offer the following comments related to issues raised in the committees’ letter.

Patch Availability is not Patch Deployment

The committees’ letter asks “...whether companies used precise terminology in describing the availability, not application, of patches” and points out “...the misapplication of such terms as ‘in place’ and ‘available’ when used to describe the status of vulnerability patches.”

CVD guidance can be more clear in both terminology and the boundary between the phases of patch availability and patch deployment. And while we agree that vendors should take care not to overstate the status of patch deployment, the best many vendors can do today is to make patches available, along with sufficient vulnerability information for users to make informed patching and other risk

³ <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330>

decisions.⁴ Ultimate responsibility for installing patches often falls to deployers,⁵ including end users.

While we appreciate the committees' desire that "sound CVD strategies would seek to limit disclosure of vulnerability information before stakeholders are able to apply patches," our experience indicates that it is impractical to privately notify all affected stakeholders without public disclosure. Thus, public disclosure is usually the best practice to inform affected parties—including end users—who may need to take action in order to apply patches to their software and devices.

The committees' letter correctly points out that the deployers' need to test patches "can lead to a lag time of weeks or months before a patch is applied." We note that in the extreme, this lag time can become indefinite for reasons including:

- Some deployers (including many end users) will remain unaware of the availability of patches, or will lack the technical capability to deploy them successfully.
- Long or complex supply chains for patch distribution may result in patches issued by an originating vendor not making it through to the downstream vendors' products in a timely manner.
- Some deployers will intentionally choose to accept the risk and not apply the patch at all. The decision to apply patches is a risk management decision.

For especially pervasive vulnerabilities such as Meltdown and Spectre, there is no clear optimal solution to balancing the diverse operational cadence across such a wide range of industries (including critical infrastructure sectors) with the need for timely public disclosure. It may be that the best we can expect is for consistent, accurate, thorough, and timely information to be provided in support of defender decisions.

Vendor, Coordinator, and Government Relationships

During the CVD process, there is an important focus on privately notifying organizations, primarily vendors, who have the ability to create patches to fix vulnerabilities. Some vendors are multinational organizations, and some vendors are headquartered or incorporated outside of the United States. In multiparty CVD, it is impractical to *not* notify foreign vendors, and furthermore it is often necessary to inform foreign vendors in order to produce patches for software and devices used in the United States. It is also impractical for those acting as coordinators to keep track of a myriad of vendor relationships to foreign governments. Similar concerns are echoed in recent negotiations to provide security research and international CVD exemptions for the Wassenaar Arrangement.⁶

The focus on producing patches should not come at the expense of notifying organizations responsible for critical infrastructure protection and public safety—typically government organizations like

⁴ Some products have secure, robust, and automated patch deployment features. Software-as-a-service (SaaS) and other cloud services can typically be updated by providers, requiring little if any action by end users.

⁵ By "deployers" we mean those responsible for choosing if, when, and how to install patches or perform other mitigating or compensating actions. Deployers can include system administrators, vulnerability management systems, vendors with the ability to push patches, and end users who must take manual action.

⁶ <https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research>

DHS NCCIC (including US-CERT and ICS-CERT). We consider the vendors' lack or inadequacy of such notification to have been in error.

Furthermore, some vendors have expressed to us their concerns that inclusion of DHS NCCIC in CVD processes could lead to leaks or even exploitation by other U.S. agencies. We believe these concerns to be specious, as we are not aware of any embargoed vulnerabilities reported to DHS NCCIC having been leaked prematurely. Also, the U.S. Vulnerability Equities Process (VEP) explicitly places vulnerabilities reported to the government under CVD out of scope: "Vulnerabilities identified through security researcher activity and incident response that are intended to be disclosed in a rapid fashion will not be subject to adjudication by the VEP."⁷

In multiparty CVD, private notifications to other vendors and even public disclosures by individual vendors may not sufficiently raise awareness or accurately reflect the scope of a vulnerability. Because of the role they play in conveying information to a broad audience of system deployers, trusted third parties (non-vendors) such as DHS NCCIC, the CERT/CC, or other coordinators can help notify affected vendors, facilitate technical analysis of the vulnerability and its impact, and amplify communications to the public.

When vendors provide advance notice of major vulnerabilities to the coordinator community, it allows the various coordinating organizations to prepare accurate remediation instructions for system deployers, and to publish that information in synchronization with the vendors' release of the patches. When that advance notification does not occur sufficiently early,⁸ as in the case of Meltdown and Spectre, coordinators may be in a rush to understand the issue while preparing their advisories, leading to erroneous or inadequate advice to their constituencies.

Internet of Things Security Maintenance

Although indirectly related to the Meltdown and Spectre vulnerabilities, we wish to emphasize the need for Internet of Things (IoT) vendors to include security maintenance as an integrated part of their product and service offerings. Consumers cannot be expected to have access to the cybersecurity and information technology skills needed to keep their home and small business networks secure from common attacks. This responsibility largely falls to vendors and providers, who should consider fully automating the secure deployment of patches to consumer-grade devices.⁹ Automatic update mechanisms can greatly reduce the time between patches being available and patches being deployed.

Adding software and connectivity to durable goods implies the need for vendors to maintain the capability to address cybersecurity vulnerabilities in those goods for the duration of the products' expected lifespan, which may be considerably longer than the span of market availability of those products. Refrigerators, washing machines, door locks, cars, and even home routers can be expected

⁷ whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

⁸ In cases where a coordinator is acting as an amplifier and aggregator for public disclosure, a few weeks' notice is probably sufficient. The more engaged the coordinator needs to be, the more lead time is necessary.

⁹ <https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security>

to have usable life spans of 5, 10, even 20 years or more. Whereas it is not unreasonable to expect vendors to provide spare parts for years or even decades after the products are no longer available new, consumers may be forced to choose between living with their devices in a state of perpetual insecurity or facing the expense of replacing otherwise functional mechanical hardware just because the software no longer receives patches to protect against extant cybersecurity threats.

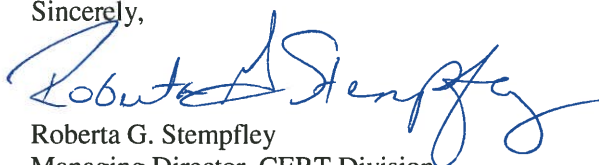
Senate bill S.1691, the *Internet of Things (IoT) Cybersecurity Improvement Act of 2017* includes clauses that require secure update features and security support that matches the expected lifetime of durable IoT products.¹⁰ For some classes of relatively less expensive IoT devices, physical replacement may be a viable mechanism for deploying security patches. At a minimum, security maintenance provisions and timelines should be clearly documented so that users can make informed purchasing and risk decisions.

Given the newfound attention directed at hardware-related side-channel vulnerabilities, it seems likely that there will be additional discoveries announced in the coming months. The complexity of fixing these vulnerabilities will likely lead to significant impact on chip manufacturers who are already redesigning new processors with better protections against these kinds of vulnerabilities. Because of the significant lead time required for such design, we expect these vulnerabilities to be present in the market for potentially years to come.

Looking back on the Meltdown and Spectre disclosures, we first recognize the continued need to improve multiparty CVD guidance. Second, there is an opportunity to clarify the language used to convey patch status. Third, given industry and governments' shared interest in protecting critical infrastructure and consumers, public disclosure could be improved with earlier engagement of key stakeholders, particularly for significant vulnerabilities like Meltdown and Spectre. Fourth, IoT vendors should provide adequate security maintenance for the lifespan of their products. Finally, software engineering practices such as threat modeling and focused security testing can help vendors reduce the number of vulnerabilities they release.

We intend to continue working to improve CVD processes both within the U.S. and globally, and we appreciate the opportunity to provide our comments to your committees.

Sincerely,



Roberta G. Stempfley
Managing Director, CERT Division
Software Engineering Institute

¹⁰ <https://www.congress.gov/bill/115th-congress/senate-bill/1691>

