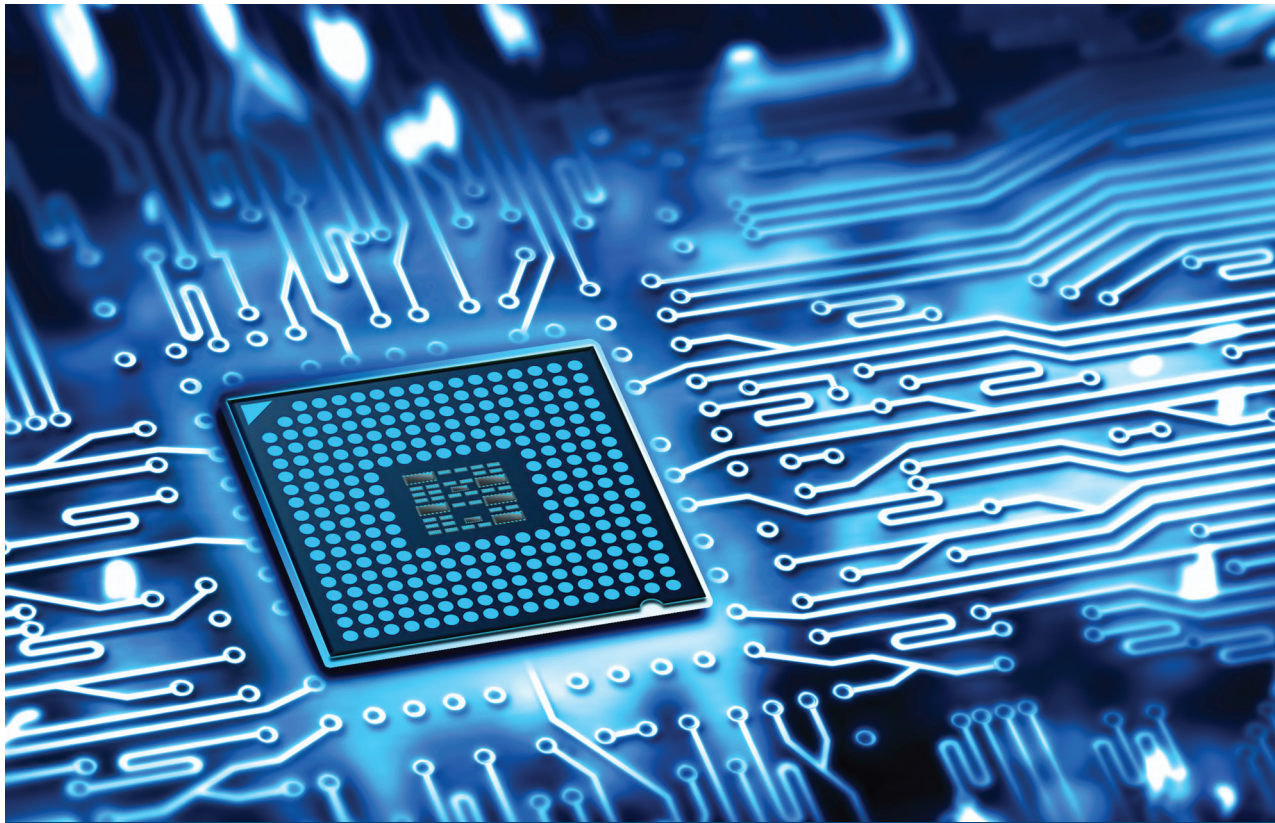


# Improving Hardware Component Vulnerability Disclosure



The Center for Cybersecurity Policy and Law

April 2019

## FOREWORD

Reader,

It is not a question of whether we can expect technologies to have vulnerabilities. We know they will. The question is how do we minimize the damage that exploiting those vulnerabilities can do. Of course this means finding more vulnerabilities before the technology is released, but it also means responding quickly and efficiently when researchers find vulnerabilities in already released technologies.

This report focuses on vulnerabilities in hardware components. Over the last decade, industry has made great strides on both software and hardware vulnerability reporting, and in building trust between companies and researchers. But because we have had fewer major hardware vulnerabilities, there has been less focus on some of the unique aspects of hardware vulnerability disclosure and how to improve it.

Addressing these challenges is essential to the security of our networked economy. To be successful, the path forward must be based on international standards and informed by reality. It is my hope that through the work of the Center and its many partners, we can continue the conversation on how hardware vulnerabilities impact us today, and how we can continue to work together to continually improve how we respond to new vulnerabilities that could impact the safety and security of people around the world.

Sincerely,

A handwritten signature in black ink, appearing to read 'A. Schwartz'.

Ari Schwartz  
*Executive Coordinator,  
Center for Cybersecurity Policy and Law*

## EXECUTIVE SUMMARY

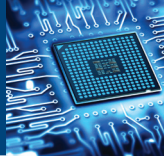
Coordinated Vulnerability Disclosure (CVD) is a standardized, multi-step process through which stakeholders identify, develop, validate, distribute, and deploy mitigations for security vulnerabilities. Historically, CVD has been focused primarily on software vulnerabilities. With the rapid growth and variety of connected devices however, there is increasing interest in hardware component vulnerabilities. This paper outlines ways in which hardware component vulnerabilities differ from those in software CVD processes. Three important such differences are:

- The fact that hardware mitigations may require action at multiple system layers;
- The larger number of participants often required to develop, test and deploy mitigations addressing hardware vulnerabilities; and
- The potential for reliance on third parties for distribution of mitigations addressing hardware vulnerabilities.

To address these and other challenges, we offer the following recommendations:

- ***The primary goal of CVD - whether describing vulnerabilities in software or hardware - is reducing end user risk and enhancing end user security. That primary goal is best accomplished when stakeholders work together to mitigate vulnerabilities in a responsible and coordinated manner.***
- ***Likewise, CVD should limit involvement to persons necessary to develop, validate and deploy a mitigation.***
- ***Hardware and software vendors should collaborate and iterate to streamline the deployment of patches and other mitigations as quickly as possible.***
- ***Hardware vendors should work with partners on effective enforcement of disclosure embargos and other measures to protect the agreed-upon process.***
- ***Hardware vendors should develop educational tools and conduct outreach to policymakers to inform their understanding of hardware vulnerabilities and CVD processes.***
- ***Hardware vendors should work on initiatives to increase the adoption rate of mitigations for known hardware vulnerabilities.***

It is clear that vulnerabilities will continue to be found in hardware in the future. These recommendations will help hardware vendors to evolve multiparty CVD to minimize risks for end users.



## INTRODUCTION

There are security researchers that actively seek out vulnerabilities in technology, there are researchers that work to build defenses, and there are security researchers who do a little bit of both. As technology has become more complex and our business and personal lives increasingly rely on a wide array of interdependent hardware and software technologies, security researchers will continue to play an essential role in improving the security of products, data, and even personal safety when they bring to light and help mitigate risks posed by known and unknown security vulnerabilities.

Coordinated Vulnerability Disclosure (CVD) offers a well established process for researchers — both those focused on adversarial testing and those focused on protections — to work together toward this goal. Theoretically, CVD works the same way for both software and hardware. However, there are several practical factors that create a different set of challenges when dealing with hardware vulnerabilities.

First, the regularity of updates to address software vulnerabilities has created an understating and awareness among users and enterprises alike about the process for receiving those updates. Conversely, hardware vulnerabilities and what is entailed from a CVD perspective to address them, is less broadly understood or explored. In part, this is because there are so many fewer hardware vulnerabilities than software vulnerabilities. Our research showed that only about one in ten vulnerabilities reported are hardware vulnerabilities.<sup>1</sup>

Also, efforts to mitigate hardware security vulnerabilities frequently require the participation of a broad set of stakeholders, including manufacturers, suppliers, and technicians, each of whom has a role to play in identifying the vulnerability, developing, testing, distributing the mitigation, and ensuring that mitigation is deployed correctly, securely and quickly.



Hardware makes up about  
1 in 10  
reported vulnerabilities.

Below we provide detail on exactly what makes hardware different in this area and offer a number of recommendations specific to the hardware environment, with the goal of advancing the shared objective of reduced end user risk and enhanced end user security.

## COMPLEXITIES IN MITIGATING VULNERABILITIES

The threat posed by security vulnerabilities has grown over time as digital technology has become increasingly integrated in all aspects of the modern world, and the complexity of systems has grown. With the proliferation of connected devices that are dependent on applications, code libraries, and hardware components, a single vulnerability in a piece of code or hardware has the capacity to affect a large number of organizations and individuals worldwide. Some vulnerabilities have limited impact and are easily mitigated. Others may have broader implications.

---

<sup>1</sup>We reviewed the records in the National Vulnerability Database (NVD) between December of 2018 and February of 2019. Unfortunately, NVD does not clearly indicate whether something is hardware or software, but based on the information in the record we found somewhere between 7.5-12.5 percent of all recorded vulnerabilities were related to hardware. We are averaging this finding out to “about 1 in 10.”



One example of a wide ranging software vulnerability is Heartbleed.<sup>2</sup> Disclosed in April of 2014, Heartbleed was found in OpenSSL, an open-source cryptographic library used extensively to provide encrypted communications for website, email, and other Internet protocols. Heartbleed is a relatively easy vulnerability to exploit, so the race to find a mitigation became urgent. As with many software vulnerabilities however, the process to mitigate was likewise relatively straightforward: update the vulnerable libraries and make them available for users to integrate in their software products.

That path is often not possible in the case of some hardware vulnerabilities. This was recently demonstrated by exploits popularly referred to as Spectre and Meltdown.<sup>3</sup> Disclosed in January 2018, Spectre and Meltdown take advantage of a feature called *speculative execution* common to most modern processor architectures. In many ways, Spectre and Meltdown proved to be the opposite of Heartbleed. They are relatively difficult to exploit, and there have been no known exploits to date using these vulnerabilities. The Spectre and Meltdown proof of concept demonstrated that when specific, targeted malware is created and implanted in a system, a malicious attacker could leverage speculative execution to infer data values that would normally be protected. The process for mitigating Spectre and Meltdown however, demonstrates the complexity in coordination that can be required to address many hardware vulnerabilities.

Mitigation of a hardware vulnerability may require patches to microcode/ firmware, as well as the operating system, or other system software. In the case of Spectre and Meltdown, affected vendors took different approaches based on their respective architecture, and the variant of the vulnerability.<sup>4</sup> This increased the complexity of the situation and required unprecedented collaboration across the industry to develop, test, and deploy mitigations.

In particular, this example raises the question of how mitigations in a complex multi-party environment are distributed to end users and highlights why the response can be much more complex than those involving traditional software vulnerabilities. When microcode updates are required, distribution has historically occurred not through the processor manufacturer directly, but rather through the Original Equipment Manufacturers (OEMs), the brand name company of the assembled device, in which the processor is a component. Distribution can also be accomplished in some cases through the operating system (OS) vendors and/or directly to cloud providers. In all cases, these updates must be tested and validated by all parties on their potentially affected product lines and services before distribution.

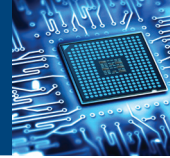
The shared risk created by vulnerabilities in widely used products requires a coordinated response that crosses borders and businesses. CVD has worked well — but by its nature, requires agreement and cooperation on the proper processes, particularly in the complex situations that can ensue. Hardware component vulnerabilities often present such situations where multiparty CVD is key to mitigate users' risk, yet industry norms and CVD processes are still developing.

---

<sup>2</sup> <https://nvd.nist.gov/vuln/detail/CVE-2014-0160>

<sup>3</sup> <https://nvd.nist.gov/vuln/detail/CVE-2017-5754>.

<sup>4</sup> For example, AMD released OS and Microcode updates <https://www.amd.com/en/corporate/speculative-execution-previous-updates#paragraph-337801>; ARM made firmware updates available [https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability?\\_ga=2.252673869.599477536.1553528979-1913652762.1553286604](https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability?_ga=2.252673869.599477536.1553528979-1913652762.1553286604); Intel responded with both OS and Firmware mitigations and <https://www.intel.com/content/www/us/en/support/articles/000031501/processors.html>



A bug bounty program provides incentives that can be either financial, reputational or other for external researchers to discover vulnerabilities using lawful means and report them under agreed terms, which will often include a CVD requirement. Bug bounty programs have gained traction as a means to increase the number of skilled researchers looking for vulnerabilities.

## COORDINATED VULNERABILITY DISCLOSURE (CVD)

CVD is a process to guide vendors, researchers and other potential stakeholders in the complex task of vulnerability reporting, analysis, mitigation and disclosure. The primary goal of CVD—for software and hardware vulnerabilities alike—is to protect end users from exploitation. CVD is driven by the understanding that disclosure of a vulnerability before a mitigation is available makes exploitation more likely. Current CVD policies and practices try to strike a balance that promotes the swift development, testing, and implementation of mitigations while reducing the likelihood of premature disclosure by including only those stakeholders that are absolutely necessary at each stage.

## MULTIPARTY HARDWARE COORDINATED VULNERABILITY DISCLOSURE

Hardware and software vulnerabilities are different in important ways. Three distinct—but related—factors principally differentiate them, and how their mitigations are coordinated.

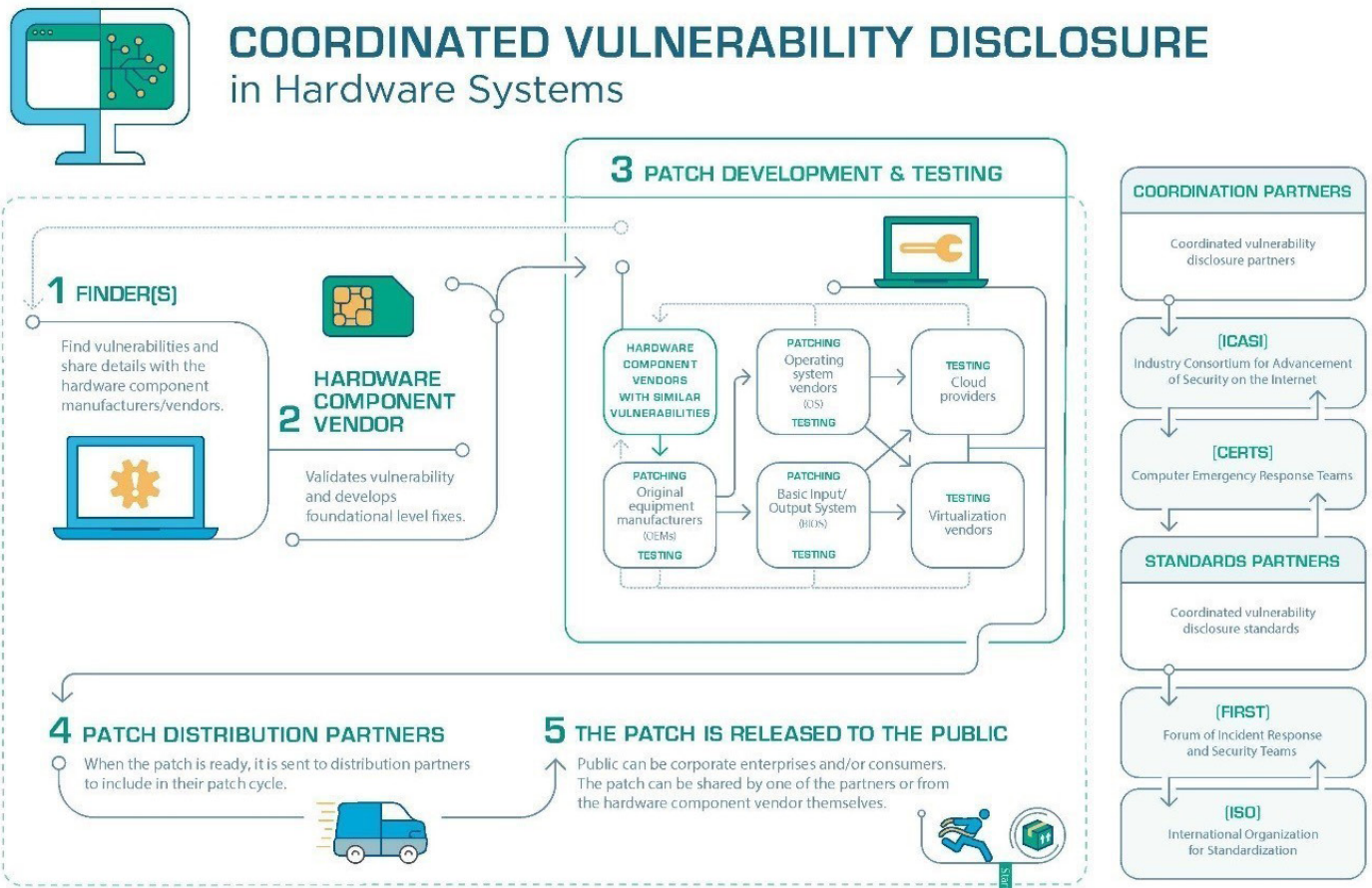


Figure 1 (Coordinated or Vulnerability Disclosure in Hardware Systems)



1. **Hardware vulnerabilities more often require multiparty coordination.** Unlike in the context of software, where a single or small number of participants may be able to develop, validate and deploy mitigations effectively, hardware vulnerabilities commonly require the active participation of multiple stakeholders, including:

*Hardware Vendors:* Where a vulnerability is identified in a piece of hardware, that vendor traditionally takes the lead in bringing together the necessary stakeholders and in the overall process, at least until stage 4 in Figure 1 (distribution of the mitigation).

*Original Equipment Manufacturers (OEMs):* OEMs are companies that assemble hardware and software components into end user products. OEMs often create their own BIOS and firmware to be compatible with their products. In those cases, an update to the microcode of a particular CPU used in an OEM's product must be tested and validated with that OEM's unique configuration. Hardware updates are typically provided to end users through OEMs, which are more likely to have direct or indirect relationships with the end users.

*Operating Systems/Firmware Vendors:*<sup>5</sup> OS/firmware vendors commonly play a central role in developing, testing, and distributing software-based mitigations (which may be important parts of the mitigation strategy for hardware vulnerabilities). This group includes the open source community who may maintain essential code used by the OS as well as hardware component drivers.

*Virtualization Vendors:* Virtualization software is a separate but important layer of the computing stack that requires consideration both when mitigations are in development and during testing for deployment. Mitigation of hardware vulnerabilities often requires updates to virtualization software.

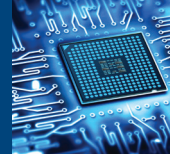
*Cloud Service Providers (CSPs):* CSPs play a significant role in the research, development, and testing mitigations for hardware vulnerabilities that impact the technological infrastructure they operate and maintain. Larger CSPs also have the computing resources to help test mitigations "at scale"—i.e., simulating widespread deployment of a mitigation.

2. **Mitigations for hardware vulnerabilities may require action at multiple system layers**

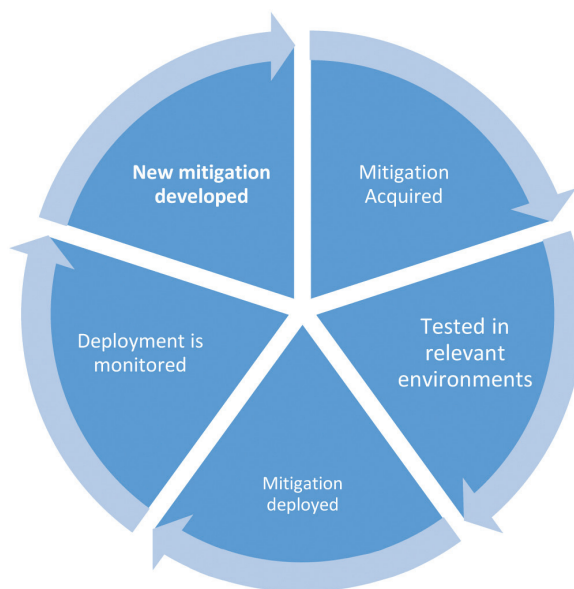
As was the case for the response to Meltdown and Spectre, addressing a hardware vulnerability is often more complex than simply developing and distributing a patch. Step 3 in Figure 1 shows some of that interplay. Initial response efforts may involve temporary mitigations while more permanent solutions are developed. Also, the nature of a mitigation may depend on how the hardware component at issue has been integrated with other systems, the environment in which it has been deployed, and the operating systems and applications running on it.

---

<sup>5</sup> We recognize that there are differences between operating systems and firmware, but have grouped them together here, as the role they play in the CVD process is functionally equivalent.



Practically speaking, this means that mitigations may be developed, produced, tested, distributed and deployed in any number of ways. It also means that testing of mitigations for hardware vulnerabilities is complex and time consuming, where the many organizations involved are likely to have different internal processes that take different forms and varying lengths of time. In hardware component vulnerabilities the mitigation development process will often require multiparty coordination, even in cases where a single component vendor is the party actively developing the solution.



*Figure 2: Mitigation Testing Process*

**Figure 2** shows a high level outline of a typical internal mitigation process. Such processes generally repeat internally, with results coordinated across other partners, until the mitigation is ready to be released.

### 3. Hardware vendors often rely on others for mitigation distribution

A hardware manufacturer's ability to deploy a patch or other mitigation depends on how the product is integrated into assembled products. For example, a component vendor typically has no direct path to end users, meaning that a mitigation will need to involve the OEM at a minimum. On the other hand, if a vendor is producing all the components for a device, including the software/firmware, the vendor may be able to address problems on its own.<sup>6</sup>

These factors may cause multiparty hardware vulnerability disclosure to be more complex than the process for software. This complexity can result in variable timeframes for completing the CVD process. Adding to the difficulty in these processes, the current standards and best practices for CVD describe single vendor coordination in far more detail than multiparty coordination. As with all CVD, the goal is to provide mitigations for a vulnerability in the shortest possible timeframe and before public disclosure to reduce the possibility of exploitation by malicious actors. The longer any vulnerability is unmitigated, the more likely it becomes that malicious actors will discover and exploit it. Thus, when the timing of the hardware CVD process exceeds the norms for software vendors, pressure may grow to disclose the vulnerability. Some stakeholders may even feel compelled to take unilateral action to protect themselves or their customers. Because the goal of CVD is to reduce harm to end users, improving the alignment of stakeholders to the hardware CVD processes and helping end users deploy mitigations in a timely manner is essential. Depending on the nature of the vulnerability, disclosure in the absence of available mitigations may offer limited value, while increasing the risk for exploitation. In this respect, end users may have no or limited ability to take unilateral action that can reduce risk.

<sup>6</sup> While this circumstance remains the exception, the rise of small and relatively simple IoT and industrial control system (ICS) devices will likely increase the frequency.



## Other Parties with Potential CVD Involvement

In addition to the stakeholders described above, there are other types of groups that may not be engaged in the CVD process directly, but may play important roles:

*Standards Development Organizations:* Standards serve to formalize existing practices and supply the groundwork on which CVD is based. Two standards most commonly referenced with respect to CVD are ISO 29147 *Information technology – Security techniques – Vulnerability disclosure*<sup>7</sup> and the Forum of Incident Response and Security Teams (FIRST) *Multiparty Vulnerability Coordination*<sup>8</sup> guide.

*Governments:* Engagement with governments can be challenging. Governments are major consumers of technology and thus can be important end users. Governments must protect and may own or control critical infrastructure in their respective countries. Governments also may have significant research capabilities—they may discover vulnerabilities and share proofs of concept with a vendor and serve as the Finder in the CVD process documented above. On the other hand, national security or commercial objectives may cause governments to take advantage of vulnerabilities that have not yet been mitigated.

In a global technological environment, often vulnerabilities will impact technologies across borders. This puts vendors in the uncomfortable position of managing simultaneous engagement with multiple, potentially adversarial countries. In particular, there is a concern over the “weaponization” of the vulnerability — meaning the use of knowledge about an unmitigated vulnerability to create an exploit and gain advantage against its adversaries. Disclosure to one government inevitably creates pressure to disclose to others, both during the CVD process and after.

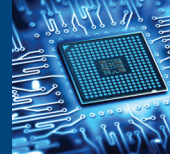
Taken together, these challenges mean that hardware vendors, like software vendors, should have a plan in place that provides guidance on how governments will be engaged, if at all, and under what circumstances. As a general matter, following the CVD principle of carefully limiting information to those involved in developing and distributing a mitigation means that governments, like everyone else not taking an essential part in the mitigation process, should not routinely receive predisclosure vulnerability information.

Finally, policy makers in governments may establish legislation and regulatory oversight directed to vulnerabilities and the CVD process, particularly as they pertain to consumer protection and critical infrastructure. Globally, policy makers need to be educated on the reasons that vulnerabilities exist in the first place; why the CVD process is both effective and essential; how CVD actually works and its complexity; the potentially distinct implications imposed on CVD by hardware and software; and how to avoid counterproductive policy measures that would increase risk to end users, render the industry-driven CVD process less effective, or that would burden innovation and slow or stall technology development and proliferation.

---

<sup>7</sup> <https://www.iso.org/standard/45170.html>

<sup>8</sup> <https://first.org/global/sigs/vulnerability-coordination/multiparty/>



## RECOMMENDATIONS

To address the particular challenges posed by CVD in the hardware context, we put forth the following recommendations:

***Recommendation 1: The primary goal of hardware CVD is reducing end user risk and enhancing end user security. That primary goal is best accomplished when stakeholders work together to mitigate vulnerabilities in a responsible and coordinated manner.***

The existing CVD process works well, and its fundamental goal should remain unchanged—all parties should be motivated to address a vulnerability as quickly as possible and in a manner that minimizes negative impact to users, safety, and security.

***Recommendation 2: Hardware CVD should limit involvement to persons necessary to develop, validate and deploy a mitigation.***

Determining the right stakeholders to involve, and when to involve them, will vary depending on the circumstances. Given the complexity of hardware vulnerabilities, the necessary stakeholders may not be limited to the ‘big players’ in the market. But maintaining tight control over knowledge of a vulnerability is essential to reduce the risk of premature public awareness and exploitation before mitigations are available. Implementing and maintaining that control should not come at the expense of releasing to the public a robust, effective, and well-tested mitigation with all due speed. Rather, hardware vendors should have policies that provide guidance on what stakeholders to involve, when, and in what way. In particular, careful consideration should be given to the role of governments. In general, following the CVD principle of limiting pre-disclosure vulnerability information to those helping to develop and distribute a mitigation will guide when and how government should be engaged.

***Recommendation 3: Hardware and software vendors should collaborate to streamline and iterate the deployment of patches and other mitigations as quickly as possible.***

The longer a vulnerability remains unaddressed, the more pressure grows to publicly disclose or even take unilateral action. Reducing the time necessary to get a mitigation out to the public helps to relieve this pressure. Continuing to improve and streamline CVD processes that address the technical and supply chain complexity associated with multiparty hardware vulnerabilities would support this goal. As discussed, the CVD process is merely the starting point. Following the release of a patch or other mitigation, it then falls to distributors and end users to ensure those mitigations are applied quickly, effectively, and securely.

***Recommendation 4: Hardware vendors should work with partners on effective enforcement of disclosure embargos and other measures to protect the agreed upon process.***

Participation in the multiparty CVD process is a voluntary activity that requires stakeholders to have confidence in each other’s intentions and actions. That confidence is essential to protect users. The benefits of coordination should be tied to behaviors that promote success of the effort and provide for consequences for those that violate trust and might put end users at risk. To be clear, this is not to suggest that hardware vendors should attempt to penalize researchers who have brought the vulnerability to the attention of the



vendor and have elected to engage in the CVD process. This recommendation is focused on the mitigation development and testing partners who have been brought into the process to help protect their users and ensure functionality of their products.

► ***Recommendation 5: Hardware vendors should develop educational tools and conduct outreach to policymakers to inform their understanding of hardware vulnerabilities and CVD processes.***

Policymakers around the world need to better understand what CVD is, how it works, its complexities, and why it is the most effective method to address multiparty hardware vulnerabilities in an increasingly complex and global technological environment. Otherwise, governments may propose and enact laws and regulations that fail to protect end users, or to adequately address national and economic security interests. In turn, hardware manufacturers and other stakeholders have a responsibility to study and understand the responsibilities and objectives of policymakers and governments, and should leverage the value that government resources may be able to contribute in encouraging mitigation deployment.

► ***Recommendation 6: Hardware vendors should work on initiatives to increase the implementation rates of mitigations for known vulnerabilities.***

Even where mitigations are developed successfully, end users do not always apply mitigations, whether because (a) they are unaware of the risk and/or that a mitigation exists; (b) they perceive that the mitigation would impact mission-critical systems in an undesirable way; or (c) they view the cost and disruption of implementing the mitigation as too great.

Also, in order to be successful, hardware vendors must improve the user interface for patches and other mitigations. To date, these type of patches have been so rare that users are already not aware or prepared to get a hardware patch, but to increase adoption, hardware companies need to actively make patching as seamless an experience as possible while still providing users an understanding of what is being done to their machine and not allowing others to exploit it.

Regardless of the reason, increasing mitigation adoption rates is a significant issue that the technology industry needs to address on multiple fronts, including by educating end users about specific vulnerabilities and, more generally, the importance of vulnerability management in enterprise risk management processes and programs.

## CONCLUSION

Technology and innovation create opportunities that drive economic growth, improve safety, security, and health care, and impact us in ways we cannot yet envision. But these benefits and opportunities also come with risks in the form of potential security vulnerabilities. In the near term, we can expect the number and severity of these vulnerabilities to increase. Addressing such risks requires the participation of every organization and user that is impacted by hardware component vulnerabilities. CVD remains an effective and increasingly important method to addressing these vulnerabilities even in complex cases, but all parties will have to continue to iterate and improve coordination to be able to step up to the new challenges we face together.



## ABOUT THE CENTER FOR CYBERSECURITY POLICY AND LAW

The Center for Cybersecurity Policy and Law<sup>9</sup> is a nonprofit (501(c)(6)) organization that develops, advances, and promotes best practices and educational opportunities among cybersecurity professionals. The Center provides a forum for thought leadership for the benefit of those in the industry including members of civil society and government entities in the area of cybersecurity and related technology policy. The Center seeks to leverage the experience of leaders in the field to ensure a robust marketplace for cybersecurity technologies that will encourage professionals, companies, and group of all sizes to take steps to improve their cybersecurity practices.

*The Center currently has three primary initiatives:*

### **Hardware-Centric Coordinated Vulnerability Disclosure Practices**

Launched in April of 2018, the Initiative brings together key stakeholders from across the technology sector to identify needs and circumstances of the hardware ecosystem, possible gaps in disclosure policy and practice, and options for future improvements.

### **The Cybersecurity Coalition**

Launched in February of 2016, the Cybersecurity Coalition works with leaders to develop consensus-driven policy solutions that promote a vibrant cybersecurity ecosystem, support the development and adoption of innovations, and encourage organizations to take steps to improve their cybersecurity.

### **The Better Identity Coalition**

Launched in February of 2018, the Better Identity Coalition is a nonprofit organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication.

