



February 7, 2018

The Honorable Greg Walden, Chairman  
Committee on Energy and Commerce  
2185 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Marsha Blackburn, Chairman  
Subcommittee on Communications and Technology  
2266 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Robert E. Latta, Chairman  
Subcommittee on Digital Commerce  
and Consumer Protection  
2448 Rayburn House Office Building  
Washington, D.C. 20515

The Honorable Gregg Harper, Chairman  
Subcommittee on Oversight and Investigations  
2227 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Walden, Chairman Blackburn, Chairman Latta, and Chairman Harper:

Thank you for your letter regarding the response by technology companies to the security vulnerabilities referred to as “Meltdown” and “Spectre.” Microsoft appreciates the opportunity to answer your questions and to address the important cybersecurity issues they raise.

By way of background, Meltdown and Spectre are the names of recently discovered vulnerabilities in the central processing unit (“CPU”) hardware that powers phones, PCs, and servers.<sup>1</sup> They are based on a common processor chip architecture that, when originally designed by hardware manufacturers, was created to increase processor speed. The attack techniques that exploit these hardware vulnerabilities could potentially be used to access sensitive data present in a computer system’s memory.<sup>2</sup> Because the hardware vulnerabilities are present in existing chips and inherent to modern chip designs, including in those made or designed by Intel, AMD, and ARM (the “chip companies”),<sup>3</sup> the chip companies have needed to

---

<sup>1</sup> See, e.g., Microsoft Windows Support, Protect Your Windows Devices Against Spectre and Meltdown, *available at* <https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown>; Terry Myerson, Microsoft Secure, Understanding the Performance Impact of Spectre and Meltdown Mitigations on Windows Systems, Jan. 9, 2018, *available at* <https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/>.

<sup>2</sup> See US-CERT, Alert (TA18-004A), Meltdown and Spectre Side-Channel Vulnerability Guidance, Jan. 4, 2018, *available at* <https://www.us-cert.gov/ncas/alerts/TA18-004A>.

<sup>3</sup> See Intel Responds to Security Research Findings, Intel, Jan. 3, 2018, *available at* <https://newsroom.intel.com/news/intel-responds-to-security-research-findings>; Information Security is a Priority at AMD, AMD, Jan. 3, 2018, *available at* <https://www.amd.com/en/corporate/speculative-execution>; Vulnerability of Speculative (continued...)

work with other companies, including operating system vendors, to develop mitigation techniques that address the vulnerabilities through a combination of chip microcode updates and software mitigations. Updates to both hardware and software are thus required to address these vulnerabilities.

The industry has not previously dealt with this type of complex hardware vulnerability, and the response, in turn, has required active engagement by a cross-section of technology companies—including not only the chip companies whose hardware contains these vulnerabilities but also the traditional software vendors. Such collaboration has been essential to finding the best measures to mitigate risk for our customers.

The response to Meltdown and Spectre has been based on an information sharing protocol known as coordinated vulnerability disclosure (“CVD”), which many technology companies have followed for more than a decade. The CVD protocol is supported by the CERT Coordination Center (“CERT/CC”), a research organization funded by the Department of Defense and the Department of Homeland Security and tasked with coordinating responses to security compromises and analyzing product vulnerabilities.<sup>4</sup> CVD is a protocol that is designed to reduce the security risks associated with vulnerabilities as companies work to mitigate them. As CERT/CC has recognized, the “ideal scenario” in mitigating a vulnerability “occurs when everyone coordinates and cooperates to protect the public.”<sup>5</sup> The CVD protocol balances the competing concerns that may arise in these circumstances.<sup>6</sup> Microsoft has long supported and adhered to CVD to minimize risk to customers.<sup>7</sup>

There are two integral entities in the CVD protocol: the finder and the owner. In this case, Google Project Zero (“GPZ”) was the finder of the Meltdown and Spectre vulnerabilities and the chip companies are the owners; Microsoft was neither. The finder of a vulnerability—here, GPZ—is the individual or organization that identifies that vulnerability. Finders often include researchers, developers, systems administrators, security analysts and others. The vendor is the individual or organization that created or maintains the product that is vulnerable and is also known as the owner of the vulnerability. Here, the chip companies are the owners. Under the CVD protocol, the owner is responsible for determining how best to address the

---

Processors to Cache Timing Side-Channel Mechanism, ARM, updated Jan. 31, 2018, *available at* <https://developer.arm.com/support/security-update>.

<sup>4</sup> See CERT Division FAQ, *available at* <https://www.cert.org/faq/>.

<sup>5</sup> See The CERT Guide to Coordinated Vulnerability Disclosure, August 2017, at 7, *available at* [https://resources.sei.cmu.edu/asset\\_files/SpecialReport/2017\\_003\\_001\\_503340.pdf](https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf) (“CERT CVD Guide”).

<sup>6</sup> *Id.*

<sup>7</sup> See, e.g., Microsoft Security TechCenter, Coordinated Vulnerability Disclosure, *available at* <https://technet.microsoft.com/en-us/security/dn467923.aspx> (“Microsoft CVD Policy”); Chris Betz, Microsoft Security Response Center, A Call for Better Coordinated Vulnerability Disclosure, Jan. 11, 2015, *available at* <https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/>.

(continued...)

vulnerability in its product. When a finder discloses the vulnerability to the owner or operator of the product, the CVD protocol then calls on the owner or operator to develop a remediation for that vulnerability. The CVD protocol explicitly provides that the finder keep the details of the vulnerability confidential until the remediation is released, so that customers are not put at risk unnecessarily.<sup>8</sup> This is because CVD recognizes the importance of getting relevant information into the public’s hands, but balances this against the danger of releasing information about a vulnerability before mitigation measures are in place.

In complicated scenarios like this one, the owner of the product or service may also need to coordinate with other providers in its supply chain to develop mitigation strategies. As CERT/CC recognizes, “[a]t its most effective, CVD follows the supply chain affected by the vulnerability.”<sup>9</sup> Under CVD, third parties (such as those in the customer supply chain) receiving information about new vulnerabilities from an owner must coordinate with that owner, and generally seek its permission, before disclosing that information to others.<sup>10</sup> If vendors do not coordinate with the owner about disclosure, they put customers at risk by increasing the possibility the vulnerability will be publicly disclosed before the owner has mitigated it.<sup>11</sup> Applying the CVD protocol to the Meltdown and Spectre vulnerabilities involves substantial complexity from a technical standpoint (including issues unique to each chip company) and is unprecedented in scope, requiring numerous organizations to synchronize their development, testing, and mitigation release processes to reduce the risk to users.<sup>12</sup>

In the cases of Meltdown and Spectre, Microsoft is not the owner of the vulnerability. Rather, it is a downstream supply chain partner that is dependent on the owners—the chip companies—to develop mitigation measures to their hardware vulnerabilities, and cooperate in the sharing of information so that additional software mitigations can be considered and developed.

With this background, we turn to your individual questions below.

### **1. Why was an information embargo related to the Meltdown and Spectre vulnerabilities imposed?**

Throughout the efforts to address Meltdown and Spectre, and consistent with CVD, Microsoft has deferred to the owners of the vulnerabilities, in this case the chip companies, as to whether to inform other companies about the vulnerabilities. As discussed above, Microsoft has long adhered to the CVD protocol, which helps ensure that industries, enterprises, and consumers—and the entire online ecosystem—remain protected from a vulnerability until its risks are mitigated. CVD requires supply chain partners to coordinate with the owners of a

---

<sup>8</sup> *Id.*

<sup>9</sup> CERT CVD Guide at 25.

<sup>10</sup> *See, e.g., Id.* at 44-49.

<sup>11</sup> *Id.* at 46-47.

<sup>12</sup> *Id.* at 44.

(continued...)

vulnerability. It has been publicly reported that GPZ was the finder of the Spectre and Meltdown vulnerabilities.<sup>13</sup> GPZ notified chip companies Intel, ARM, and AMD of the vulnerabilities, because those companies own the hardware containing the vulnerabilities. ARM notified Microsoft of the potential vulnerabilities on June 9, 2017. In the following months, Microsoft actively engaged with the chip companies and other affected companies identified by the chip companies to mitigate against the risks posed by Spectre and Meltdown. Accordingly, Microsoft's response to the Meltdown and Spectre hardware vulnerabilities was based on the protocol of CVD and dependent on the cooperation of the chip companies.

CVD generally, and as applied here, is intended to protect against security risks from malicious actors. As this incident demonstrates, the risk that a vulnerability will be exploited increases when information about the vulnerability is disclosed outside the circle of companies that the owner determines is necessary to develop mitigations, before those mitigations are delivered. Here, an apparently inadvertent statement outside of the circle in late December 2017 regarding technical issues relating to mitigation efforts underscores how premature disclosure of even small amounts of information can lead to potential attacks before mitigations are available or in place. According to one report, on January 3, 2018, just one week after an AMD engineer made a brief comment to a public discussion group about the capabilities of the company's processors relating to "speculative references," a proof of concept emerged showing how to exploit the Meltdown and Spectre hardware vulnerabilities, which rely on techniques known as speculative execution.<sup>14</sup> Because a proof of concept illustrates how bad actors could exploit the vulnerability, the companies creating mitigations for Meltdown and Spectre were compelled to expedite the release of the mitigation measures on January 3, 2018.

The point of CVD is to enable the owners of the impacted product or service to develop a remediation *before* attacks are detected or proofs of concept are available publicly. Without CVD, the public release of a vulnerability's details or proof of concept sets off a risky race against the clock to see who can release first: the attacker, with an exploit, or the owner, with a corrective measure.

## **2. What company or combination of companies proposed the embargo?**

As neither the finder nor the owner of the Meltdown and Spectre vulnerabilities, Microsoft deferred to the chip companies, as owners of the vulnerabilities, as to whether to inform other companies about the vulnerabilities. As detailed above, the CVD protocol recognizes that finders and owners have different roles and responsibilities when new vulnerabilities are identified. Finders make the initial determination about whom to notify of a

---

<sup>13</sup> See US-CERT, Alert (TA18-004A), Meltdown and Spectre Side-Channel Vulnerability Guidance, Jan. 4, 2018, *available at* <https://www.us-cert.gov/ncas/alerts/TA18-004A>; Google Project Zero, Reading Privileged Memory With a Side-Channel, Jan. 3, 2018, *available at* <https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>.

<sup>14</sup> See Russell Brandom, Keeping Spectre Secret, The Verge, Jan. 11, 2018, *available at* <https://www.theverge.com/2018/1/11/16878670/meltdown-spectre-disclosure-embargo-google-microsoft-linux>.

(continued...)

newly-discovered vulnerability. Owners, in turn, are assigned responsibility for addressing risks posed by the vulnerability. That means that owners must also make the decisions about how to remediate the vulnerability; what information to provide to others in the supply chain, if needed; where and how that information should be provided; and what measures should be taken to draw attention to resulting mitigation measures once released, including public release of the remediation and relevant communications materials.<sup>15</sup>

GPZ, as the finder of the Meltdown and Spectre vulnerabilities, controlled the timing of their disclosure. GPZ has a policy of publicly disclosing vulnerabilities 90 days after reporting them to the affected vendor, but reserves the right to move the deadline forward or backward based on “extreme circumstances.”<sup>16</sup> As the process for developing mitigations for Meltdown and Spectre unfolded, the chip companies had responsibility for determining who else to notify. Then, as the scope of the vulnerabilities became further apparent, GPZ delayed the disclosure date in consultation with Intel, AMD, ARM and other companies, including Microsoft, which the chip companies—as owners of the vulnerabilities—had brought into the mitigation process.

### **3. When was the United States Computer Emergency Readiness Team (US-CERT) informed of the vulnerabilities?**

CVD assigns to the owners of a vulnerability the authority to decide whether to notify others, including whether to notify government agencies. Because the chip companies were owners of the Meltdown and Spectre vulnerabilities, Microsoft did not notify US-CERT about the vulnerabilities. Microsoft understands that US-CERT became aware of the vulnerabilities on January 3, 2018.<sup>17</sup>

### **4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) informed of the vulnerabilities?**

As discussed above, Microsoft, under CVD, was not the owner of the Meltdown and Spectre vulnerabilities. Accordingly, Microsoft did not report these vulnerabilities to CERT/CC.

### **5. Did your company perform any analyses to determine whether the embargo could have any negative impacts on critical infrastructure sectors such as healthcare and energy that rely on affected products? If so, what were the results? If no, why not?**

No. As discussed above, Microsoft was not the owner of the Meltdown and Spectre vulnerabilities. Microsoft followed the CVD protocol, supported by CERT/CC, with respect to the scope of information-sharing relating to the vulnerabilities, including whether any analyses

---

<sup>15</sup> CERT CVD Guide at 38-39.

<sup>16</sup> See Google Project Zero, Feedback and Data-Driven Updates to Google’s Disclosure Policy, Feb. 13, 2015, *available at* <https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html>.

<sup>17</sup> See US-CERT, Alert (TA18-004A), Meltdown and Spectre Side-Channel Vulnerability Guidance, Jan. 4, 2018, *available at* <https://www.us-cert.gov/ncas/alerts/TA18-004A>.

of negative impacts on particular industry sectors would impact the breadth of information-sharing.

**6. Did your company perform any analyses to determine whether the embargo could have any negative impacts on other information technology companies that rely on affected products? If so, what were the results? If no, why not?**

As discussed above, in accordance with the CVD protocol, Microsoft deferred to the owners of the vulnerabilities with respect to the issue of what other companies should be informed of the vulnerabilities prior to public disclosure.

While in the course of analyzing the Spectre and Meltdown vulnerabilities, Microsoft determined that the mitigations it was developing (which required complex changes to core Windows operating system functionality) could cause compatibility issues with some third-party software, including antivirus software. Accordingly, Microsoft began to notify affected third-party software developers, including antivirus software vendors, through its standard channels several weeks before the planned public disclosure of the vulnerabilities. In doing so, Microsoft provided information about the forthcoming security updates and the steps that recipients of those updates, including third-party software developers, needed to follow to implement the updates. Because the vulnerabilities were not yet public, and consistent with the best practices for CVD, Microsoft did not specifically disclose what Windows code was changed, nor the reasons why the changes were made. Nor did Microsoft disclose the specific vulnerabilities that were the underlying reason for the code changes. Similarly, to enable testing of the Windows mitigations by third-party software developers and in environments, configurations, and against applications that cannot be easily duplicated at Microsoft, Microsoft included them in pre-release security update packages and in pre-release builds of Windows 10 that were distributed through its standard partnership programs several weeks before public disclosure of the vulnerabilities. This provided third-party software vendors time to ensure their software would be compatible with the Windows mitigations when they were released following public disclosure of the Spectre and Meltdown vulnerabilities.

In addition, and again in accordance with the CVD protocol, during the process of developing mitigations for the Spectre and Meltdown vulnerabilities, Microsoft (as part of its consultation and coordination with the chip companies) also discussed mitigation strategies and timing issues with the other companies that were involved in developing mitigations, after those companies were made aware of the vulnerabilities by the chip companies.

**7. What resources or best practices did your company use in deciding to implement the embargo?**

As discussed earlier, GPZ was the finder and the chip companies were the owners of the Meltdown and Spectre vulnerabilities; Microsoft was neither. Accordingly, Microsoft did not control the decision about when and how to release information about the vulnerabilities to the public. In responding to the hardware vulnerabilities, Microsoft adhered to the best practices embodied in CVD. Consistent with that protocol, Microsoft sought to foster cooperation among entities in the supply chain best positioned to mitigate the risks posed by these vulnerabilities.

## **8. What resources or best practices did your company use in implementing the embargo itself?**

As noted above, Microsoft adhered to the best practices embodied in the CVD protocol in addressing the Meltdown and Spectre vulnerabilities.

CERT/CC has recognized that direct communications between vendors is desirable in large coordination efforts where efficient communication is needed.<sup>18</sup> In less complicated scenarios, the CVD protocol calls for a hub-and-spoke model of communication through which a vulnerability owner communicates individually with each affected vendor.<sup>19</sup> In more complicated scenarios—like the one presented by Meltdown and Spectre—a “shared-bus” model can be required, to ensure affected companies can coordinate directly “through the use of conference calls, group meetings, and private mailing lists.”<sup>20</sup>

Here, Microsoft concluded that the complexities of Meltdown and Spectre were best addressed through assisting the owners by collaborating directly with affected companies (to which the owners had disclosed the vulnerabilities) on mitigation efforts. This collaboration was exemplified by in-person discussions facilitated by Microsoft at which vendors shared their research on the vulnerabilities and discussed potential mitigation measures. The chip companies, as the owners of the vulnerabilities, determined which vendors joined these collaborative discussions, based on each vendor’s ability to contribute to and implement mitigation strategies.

## **9. Based on your company’s experience during this process, has your company established lessons learned relating to multi-party coordinated vulnerability disclosure? What are they?**

Microsoft recognizes that policies for vulnerability disclosure must reflect a balance between timely disclosing information to consumers and keeping that information confidential until mitigations can be implemented. Maintaining this balance is a complex question and we believe the CVD protocol addresses it appropriately. We recognize, however, that this is an important issue that warrants discussion and Microsoft would welcome the opportunity to contribute to such discussion. In particular, we recognize that responding to hardware vulnerabilities such as Meltdown and Spectre must be rooted in a variety of important considerations, including among others:

- the severity and complexity of the vulnerability itself, the engineering resources needed to mitigate;
- the real-world impact on customers;
- the number of supported platforms in which the issue exists;
- the complexity of the mitigations;

---

<sup>18</sup> See CERT CVD Guide at 47-48.

<sup>19</sup> *Id.* at 47.

<sup>20</sup> *Id.*

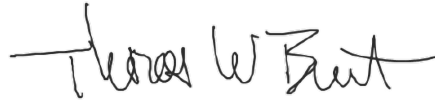
- the need to ensure those mitigations actually work (and, in this instance, because of the supply chain, that the mitigations actually work with mitigations from other vendors);
- the need to produce mitigations promptly and before bad actors exploit the vulnerabilities; and
- the need for strict confidentiality until the mitigations are ready so that customers are not placed at greater risk.<sup>21</sup>

Microsoft appreciates and recognizes the positive collaboration and information-sharing underlying this response and believes it contributed significantly to the mitigation of risk for the computing ecosystem.

\* \* \*

Microsoft appreciates the opportunity to provide the Committee with this information about the Meltdown and Spectre cybersecurity vulnerabilities. We hope that this written response has addressed your questions, but if the Committee would still like to schedule a briefing on these issues, or if we can be of any further assistance to the Committee, please do not hesitate to let us know.

Sincerely,

A handwritten signature in black ink that reads "Tom Burt". The signature is written in a cursive, slightly slanted style.

Tom Burt  
Vice President and Deputy General Counsel

---

<sup>21</sup> See Chris Betz, Microsoft Security Response Center, A Call for Better Coordinated Vulnerability Disclosure, Jan. 11, 2015, *available at* <https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/>; CERT CVD Guide at 37-38.