February 15, 2018

Mr. Jeffrey P. Bezos
President, Chief Executive Officer,
and Chairman of the Board
Amazon.com, Inc.
410 Terry Avenue North
Seattle, WA 98109

Dear Mr. Bezos:

Academic and independent security researchers,\(^1\) some of whom were federally-funded,\(^2\) recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.\(^3\) These side-channel vulnerabilities,\(^4\) which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.\(^5\)

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,” while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

\(^1\) Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.


International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Tim Cook
Chief Executive Officer
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Dear Mr. Cook:

Academic and independent security researchers,\(^1\) some of whom were federally-funded,\(^2\) recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.\(^3\) These side-channel vulnerabilities,\(^4\) which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.\(^5\)

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”\(^6\) while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

---

\(^1\) Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.


International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

[Signatures]

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Jensen Huang
President and Chief Executive Officer
NVIDIA Corporation
2788 San Tomas Expressway
Santa Clara, CA 95051

Dear Mr. Huang:

Academic and independent security researchers,\(^1\) some of whom were federally-funded,\(^2\) recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.\(^3\) These side-channel vulnerabilities,\(^4\) which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.\(^5\)

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”\(^6\) while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

\(^1\) Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.


International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---

4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Brian M. Krzanich  
Chief Executive Officer  
Intel Corporation  
2200 Mission College Boulevard  
Santa Clara, CA 95054

Dear Mr. Krzanich:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

---

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO).\textsuperscript{7} These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face.\textsuperscript{8} They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities.\textsuperscript{9} Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities.\textsuperscript{10} As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Satya Nadella
Chief Executive Officer
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Dear Mr. Nadella:

Academic and independent security researchers,1 some of whom were federally-funded,2 recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.3 These side-channel vulnerabilities,4 which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.5

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”6 while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

---

1 Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented, given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---

4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

[Signatures]

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Sundar Pichai
Chief Executive Officer
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---

4. If you communicated with a U.S. government entity regarding these vulnerabilities prior
to the date the vulnerabilities were publicly disclosed, what was the result of your
communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to
mitigate or patch these vulnerabilities in your products? Have you seen performance
impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If
not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such
exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce
cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you
think the U.S. Government should take in addressing hardware vulnerabilities or in
response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than
March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Chuck Robbins
Chairman and Chief Executive Officer
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

Dear Mr. Robbins:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

---

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities; including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Ms. Virginia M. Rometty
Chairman, President, and
Chief Executive Officer
International Business Machines Corporation
1 New Orchard Road
Armonk, NY 10504

Dear Ms. Rometty:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---

4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE  
Chairman

BILL NELSON  
Ranking Member
February 15, 2018

Mr. Simon Segars
Chief Executive Officer
ARM Holdings PLC
150 Rose Orchard Way
San Jose, CA 95134

Dear Mr. Segars:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Dr. Lisa Su
President and Chief Executive Officer
Advanced Micro Devices, Inc.
2485 Augustine Drive
Santa Clara, CA 95054

Dear Dr. Su:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---

4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Yang Yuanqing
Chairman and Chief Executive Officer
Lenovo Group Limited
1009 Think Place
Morrisville, NC 27560

Dear Mr. Yuanqing:

Academic and independent security researchers,\(^1\) some of whom were federally-funded,\(^2\) recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.\(^3\) These side-channel vulnerabilities,\(^4\) which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.\(^5\)

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU [central processing unit] bugs ever found,”\(^6\) while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

---

\(^1\) Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.


International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member
February 15, 2018

Mr. Ren Zhengfei
Deputy Chairman of the Board
and Chief Executive Officer
Huawei Technologies, Co., Ltd.
c/o Huawei Technologies USA
5700 Tennyson Parkway Suite 500
Plano, TX 75024

Dear Mr. Zhengfei:

Academic and independent security researchers,¹ some of whom were federally-funded,² recently discovered three vulnerabilities in modern computer processors that have existed for more than two decades.³ These side-channel vulnerabilities,⁴ which researchers have named “Meltdown” and “Spectre,” could allow sophisticated hackers access to stored passwords, encryption keys, and other highly sensitive information.⁵

According to one of the researchers, the Meltdown vulnerability is “probably one of the worst CPU bugs ever found,”⁶ while Spectre, although arguably more difficult to exploit, presents more significant challenges to mitigate or patch. For years, the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce has been concerned with such side-channel attacks and their impact on cryptography. In 2011, NIST held a testing workshop and coauthored standards in cooperation and accordance with the

¹ Affiliated with Google’s Project Zero, Graz University of Technology, University of Pennsylvania, University of Maryland, University of Adelaide, Cyberus, and Rambus.
International Organization for Standardization (ISO). These types of novel hardware vulnerabilities may represent the future of the potential cybersecurity risks we face. They have few countermeasures, and the scope of these vulnerabilities is unprecedented given the number of organizations and products affected.

While we recognize industry’s coordinated response to this ubiquitous, complex problem, some security experts have been critical of the process to disclose and mitigate these vulnerabilities. Although security researchers initially informed certain companies of the vulnerabilities in June of 2017, the vulnerabilities were not widely disclosed until January of 2018. In addition, a handful of Chinese customers, but not the United States government, were initially informed as part of the coordinated response, raising questions as to whether a foreign government or malicious actors could have exploited the vulnerabilities. As such, the full picture of the impact of these vulnerabilities, including who is affected, when they knew, with whom they communicated, and what steps they have taken in response, is far from clear.

The Senate Commerce Committee has previously sought to reduce cybersecurity risks through the encouragement of public-private partnerships to share cyber threat information and best practices and the promotion of cybersecurity research and standards development. Cybersecurity remains a priority for the Committee, and we request written responses to the following questions as the Committee looks for lessons and recommendations to be better prepared to address cybersecurity risks associated with these vulnerabilities in the future:

1. When and how did you first become aware of these vulnerabilities?

2. Which of your products are affected by these vulnerabilities and how are they affected?

3. Did you communicate with any entity outside your company, including any U.S. or foreign government agencies, regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed? If so, please identify each such entity and when you communicated with them.

---


4. If you communicated with a U.S. government entity regarding these vulnerabilities prior to the date the vulnerabilities were publicly disclosed, what was the result of your communication?

5. What steps have you taken to mitigate or patch these vulnerabilities?

6. What is the status of user implementation of the steps you have taken or recommended to mitigate or patch these vulnerabilities in your products? Have you seen performance impacts associated with any patches?

7. Do you believe the patches that have been released fully mitigate the vulnerabilities? If not, please identify any issues that are not fully mitigated by current patches.

8. Can you detect if these vulnerabilities have been exploited and, if so, have any such exploitations occurred, to the best of your knowledge?

9. To what degree are you coordinating your response with other companies?

10. Do you have recommendations for further or future steps to be taken to reduce cybersecurity risks stemming from hardware vulnerabilities? What role, if any, do you think the U.S. Government should take in addressing hardware vulnerabilities or in response to their discovery?

We look forward to receiving your written response as soon as possible, but by no later than March 1, 2018. Thank you for your consideration of this request.

Sincerely,

JOHN THUNE
Chairman

BILL NELSON
Ranking Member