Hewlett Packard Enterprise

Report

HPE Customer Guidance Pack: Mitigating the industrywide microprocessor vulnerability

Last Updated: 21 March 2018

Contents

All Intel-based HPE Gen10, Gen9, Gen8, G7, and G6 Server System ROMs now available

As of 19 March 2018, new System ROMs for all Intel®-based HPE Gen10, Gen9, Gen8, G7 and G6 servers have been posted to the HPE Support Website. HPE is advising customers to update their HPE servers with the new System ROMs to mitigate risk associated with the Side-Channel Analysis vulnerabilities.

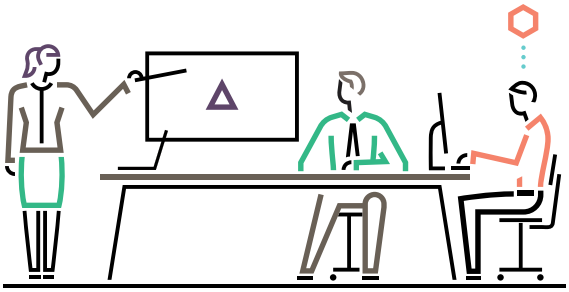
In addition, the System ROM for the AMD-based HPE ProLiant DL385 Gen10 server which includes support for mitigation of the Side-Channel Analysis vulnerabilities has been available on the HPE Support Website since early January 2018.

Intel alert: 22 January 2018

We alerted customers to an Intel statement published 22 January 2018 regarding issues associated with the Intel microcode patch designed to address the Side-Channel Analysis vulnerability that may result in "unpredictable system behavior." If HPE customers downloaded a System ROM, specific to this vulnerability, for an Intel-based server between 05 January 2018 and 21 January 2018, HPE recommends downloading the new System ROMs that are now available and updating servers accordingly.

Refer to the Intel Security Exploit Newsroom and HPE Customer Advisory for more information.

Background



Recently, an industrywide vulnerability has been identified that involves modern microprocessor architectures. Based on new security research, there are software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from computing devices that are operating as designed. Often referred to as the Side-Channel Analysis Method, or Spectre and Meltdown, this vulnerability impacts microprocessor architectures from multiple CPU vendors, including Intel, AMD, and Arm®.

To address this vulnerability, hardware and software vendors from across the industry, including HPE, have been working together to publish the appropriate resolutions. This HPE document is a guidance package for customers designed to simplify the task of mitigating risk from this vulnerability. It includes step-by-step instructions and a compilation of important links to the most common operating system (OS) and microcode updates used with the current HPE server generations. HPE also recommends that our customers review statements published by the microprocessor vendors: Intel, AMD, and Arm.

HPE customer guidance

The security of HPE products is our top priority and we continue to work proactively with OS and microprocessor vendors to develop software and firmware updates to mitigate the microprocessor vulnerability.

An important aspect of the Side-Channel Analysis Method is that it requires malware to run locally on a system. This particular vulnerability doesn't directly enable alteration, deletion, destruction, or encryption of data—but data may potentially be extracted from the computer systems. Therefore, it is important to practice good security hygiene, including always keeping your software and firmware current. Following security best practices and deploying HPE Gen10 Servers with secure Silicon Root of Trust technology can help protect your business from malicious attacks.

Recommended mitigation steps

HPE recommends all customers follow the steps for Server and Storage products below to determine their risk and mitigation plan.

For Server products:

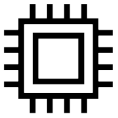
1

Determine if you have a system that is impacted by this vulnerability. HPE is maintaining a list of impacted products on the **HPE Vulnerability Website**.

2

If your system is impacted, download and install the OS update provided by the OS vendor. Depending on which system you are running, you can find instructions on appropriate actions to take in the **HPE Security Bulletin**.*

3



Update the System ROM to a revision containing an updated microcode from HPE when available. Depending on which system you are running, you can find instructions on appropriate actions to take in the **HPE Security Bulletin**.**

4

Reboot the impacted system as required, ensuring the new updates are fully deployed.

* Applying OS updates will provide protection against certain variants of the vulnerability even if System ROM updates are not available.
** If HPE customers downloaded a System ROM, specific to this vulnerability, for an Intel-based server between 05 January 2018 and 21 January 2018, HPE recommends downloading the new System ROMs that are now available and updating servers accordingly.

For Storage products:

1

Determine if you have a system that is impacted by this vulnerability. HPE is maintaining a list of impacted products on the **HPE Vulnerability Website**.

2

If your system is impacted and deemed vulnerable, follow the **Mitigation link** provided on the **HPE Vulnerability Website**.

Frequently asked questions

1. Does the microprocessor vulnerability affect all technology vendors or is this exclusive to HPE?

The microprocessor vulnerability affects all technology vendors using modern microprocessors and is not specific to HPE. All products and solutions impacted by this vulnerability require the appropriate operating system and ROM updates. Intel has stated that Itanium® processors are not impacted by the Side-Channel Analysis vulnerability.

2. Which HPE products and solutions are impacted?

Any HPE products that include affected microprocessors are potentially vulnerable. To determine if your HPE products and solutions are affected, please go to the HPE Vulnerability Website. HPE will update the list of all systems as needed.

3. Is the microprocessor vulnerability due to an active attack or breach?

No, there have been no known attacks. This microprocessor vulnerability is due to a design flaw, which when analyzed via the side-channel methodology, can enable someone to deduce data. Applying the appropriate operating system and microprocessor updates for your HPE systems mitigates the risk associated with this vulnerability.

4. What is the magnitude of the security vulnerability?

New security research identified software analysis methods that, when used maliciously, have the potential to improperly gather sensitive data from computing devices that are operating as designed. For more information, reference the following common vulnerability exposures: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754.

5. What is the resolution?

Resolution of this vulnerability requires both an operating system update, provided by the OS vendor, and a System ROM update from HPE. Depending on which HPE systems you are running, you can find instructions on appropriate actions to take on the HPE Vulnerability Website.

If you are an HPE Pointnext customer and believe you are running an impacted system, contact your Support representative.

If you are an HPE Storage customer, you can find instructions on appropriate actions to take on the HPE Vulnerability Website. HPE Storage product resolution procedures may differ from HPE server product remedies. Please consult the HPE Vulnerability Website for Storage details. For software products like StoreVirtual VSA, StoreOnce VSA, RMC, and other software titles running on x86 based servers, you are advised to refer to communications from your x86 server vendor.

6. Is it an obligation to have an active contract or warranty for downloading and installing HPE System ROM updates?

No. We are waiving the entitlement check for HPE System ROM updates for products and solutions impacted by this vulnerability, when available.

7. Which operating systems are impacted?

Windows®, Linux®, and VMware® are impacted. Operating system vendors are providing OS patching updates. Based on current communication from Intel, Itanium is not impacted and thus HP-UX, OpenVMS, and the NonStop OS on NonStop J-series and H-series systems are not affected. The NonStop OS on NonStop L-series systems run on x86 processors and are affected. In addition, the CLIMs and NSCs in NonStop systems run on x86 processors, and the Linux and Window OSs on these NonStop system components are affected. For additional information, HPE recommends contacting operating system vendors: Microsoft®, VMware, SUSE, and Red Hat®.

8. Which microprocessors are impacted?

Most microprocessors with modern architectures can be impacted by the Side-Channel Analysis Method. Intel and AMD have proactively contacted HPE and are actively working with HPE to provide resolutions. Intel has stated that Itanium processors are not impacted by the Side-Channel Analysis vulnerability. For all other microprocessor vendors, contact the processor vendor for more information.

9. Are other hardware manufacturers impacted?

All hardware manufacturers as well as public cloud service providers that use affected modern microprocessor architectures are potentially impacted. Mobile phones and client computers may also be impacted—refer to providers of those products for more details.

10. After I patch my systems, will there be an associated impact to performance?

In most cases, we expect performance impact will typically be minimal but will vary with OS and workload. HPE and our OS and microprocessor partners will continue to monitor and characterize potential performance impacts over time and provide further guidance as data is made available.

11. What does this microprocessor vulnerability mean for HPE ProLiant and HPE Synergy Gen10 servers, the World's Most Secure Industry Standard Servers?[1]

The microprocessor vulnerability is a flaw in modern microprocessors: however, there are no known attacks associated with this vulnerability. HPE Gen10 servers have the only genuine Silicon Root of Trust technology; this custom-designed silicon from HPE provides unprecedented protection from firmware attacks. Notwithstanding our enhanced security features, with regard to this particular vulnerability, customers still need to apply all recommended updates and follow security best practices.

12. What does this microprocessor vulnerability mean for customers considering buying HPE products?

You can be confident that HPE compute solutions are world-class in security and quality. The discovery of this industrywide microprocessor vulnerability, should have no impact on your decision to purchase HPE solutions. HPE will continue to work with Intel, AMD, and Arm to ensure that the resolutions needed for the microprocessors used in our products are a top priority. Furthermore, when the microprocessor updates are applied and combined with HPE's Silicon Root of Trust technology, found only in HPE Gen10 servers, our customers can be assured that their compute platform meets the industry's highest security standards.

13. Will HPE provide more updates regarding this vulnerability?

Yes, HPE will continue to post updates as more information and details become available. You can refer to the HPE Vulnerability Website.

14. HPE recently had the System ROM updates available for HPE ProLiant, HPE Synergy, HPE Superdome Flex, and HPE Superdome X server products. Why can't I find them now?

As of 19 March 2018, updates are available for all Intel-based HPE Gen10, Gen9, Gen8, G7, and G6 servers and the AMD-based HPE ProLiant DL385 Gen10 server.

On 22 January 2018, Intel published a statement regarding issues associated with the Intel microcode patch designed to address the Side-Channel Analysis vulnerability. At that time, Intel recommended that customers stop deployment of System ROMs including this microcode patch and revert to their previous version of System ROM to avoid introducing unpredictable system behavior. As a result, HPE removed existing System ROM updates for HPE ProLiant, HPE Synergy, HPE Superdome Flex, and HPE Superdome X server products from the HPE Support site.

Since that time, Intel has made revisions to the microcode and updated System ROMs are now available for all Intel-based HPE Gen10, Gen9, Gen8, G7, and G6 servers. Updated revisions of the System ROMs for other platforms will be made available by HPE after Intel provides updated microcodes.

15. Which HPE server generations will receive System ROM updates which include microcodes to enable mitigation of the Side Channel Analysis Method vulnerability?

HPE is committed to working closely with microprocessor vendors to provide System ROM updates for Gen10, Gen9, Gen8, G7, and older HPE server generations as microcode updates are made available by processor vendors.

For more information, work directly with your HPE Sales Rep or Authorized Partner for further questions and help.

[1] Based on external firm conducting cyber security penetration testing of a range of server products from a range of manufactures, May 2017.

Sign up for updates

a00039576ENW, March 2018, Rev. 2