Hewlett Packard
Enterprise

HPE Customer Guidance Pack: Mitigating the industrywide microprocessor vulnerability

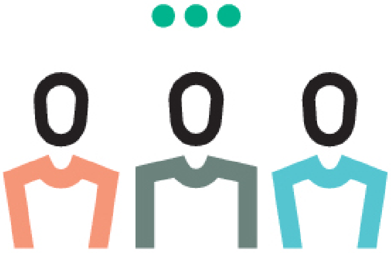
5 January 2018

Background

Recently, an industrywide vulnerability was 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.

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

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. 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.

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.

Please note that system ROM updates are available for current HPE Gen9 and Gen10 systems. We will publish updates for HPE Gen8 and older systems in the near future.

Frequently asked questions

1. **Does the microprocessor vulnerability affect all technology vendors or is this exclusive to HPE?**
   The microprocessor vulnerability is not exclusive to HPE. The vulnerability exists industrywide. All products and solutions that use microprocessors of a modern architecture are potentially impacted if a resolution hasn't been implemented.

2. **Which HPE products and solutions are impacted?**
   Any HPE products that includes affected microprocessors are potentially vulnerable. HPE products and solutions that may be affected are listed on the HPE vulnerability website. HPE will update the list as needed.

3. **Is the microprocessor vulnerability due to an active attack or breach?**
   No, there was no actual attack. This microprocessor vulnerability is due to a design flaw, which when analyzed via the side-channel methodology, can enable someone to deduce data. When the microprocessor fixes are applied and combined with the only genuine Silicon Root of Trust technology, our customers can be assured that HPE solutions are designed for an attack.

4. **What is the magnitude of the security vulnerability?**
   New security research describes 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. 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 in the HPE Security Bulletin. If you are an HPE Pointnext customer and believe you are running an impacted system, contact your Support representative.

6. **Which operating systems are impacted?**
   Windows, Linux, and VMWare are impacted. Operating system vendors are providing OS patching updates. For additional information, HPE recommends contacting operating system vendors: Microsoft, VMware, SUSE and Red Hat.

7. **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. For all other microprocessor vendors, contact the processor vendor for more information.

8. **Are other hardware manufacturers impacted?**
   All hardware manufacturers as well as public clouds that use affected modern microprocessor architectures are potentially impacted. Mobile phones and client computers are impacted—refer to providers of those products for more details.

9. **After I patch my systems, will there be an associated impact to performance?**
   In most cases, performance impact is typically minimal but varies with OS and workload. HPE and our OS and microprocessor partners will characterize the impact to performance and provide further guidance over time.

10. **What does this security vulnerability mean for HPE ProLiant and HPE Synergy Gen10 servers, the World's Most Secure Industry Standard Servers?**
    HPE manufactures the World's Most Secure Industry Standard Servers. This particular vulnerability impacts operating systems and microprocessors that our solutions use. However, HPE industry standard servers have the only genuine Silicon Root of Trust technology; Anchoring our firmware in our HPE custom-designed silicon provides unprecedented protection. Notwithstanding our enhanced security features, with regard to this particular vulnerability, customers still need to apply all recommended updates and follow security best practices.

11. **What does this microprocessor vulnerability mean for customers considering buying HPE products?**
    The discovery of this microprocessor vulnerability, which is industrywide, should have no impact on the decision to purchase HPE solutions. Customers can be assured HPE is actively working to mitigate any risk due to this vulnerability. Furthermore, when the microprocessor fixes are applied and combined with the only genuine Silicon Root of Trust technology found in HPE industry standard servers, our customers can be assured that HPE solutions are designed for an attack.

12. **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 Customer Bulletin.

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