Supply Chain Under Attack

The state of the supply chain and the ability of the US to secure it is being tested like never before in 2020. While the US has been increasingly relying on global supply, and offshoring the manufacture of many of the goods critical to our national security, the looming threat of counterfeit hardware, supply chain hacks by nation states, trade wars, and the disruption of entire industries during the COVID-19 global pandemic has brought sharp focus to the risks inherent with the status quo. Public sector agencies, financial services, healthcare, and other organizations requiring high security products are all reevaluating their reliance on globally sourced products for critical infrastructure. Leadership in the area of supply chain security is desperately needed.

HPE Trusted Supply Chain

Recognizing the growing threat to the supply chain, HPE has announced the HPE Trusted Supply Chain initiative and a Made in the US line of servers. This will start with the HPE ProLiant DL380T and will expand throughout 2021.

“Made in the US” goes above and beyond regulatory labels like “TAA-compliant”, and “Assembled in the US” which respectively allow manufacture in 126 possible countries, and where only final assembly is conducted in the US. The Made in the US label requires substantial transformation and production in the United States.

InfusionPoints conducted a broad survey of major server hardware manufacturers to determine if Made in the US servers were available. Our research suggests that today’s server hardware supply chain is murky at best. For several inquiries, inside sales conflated TAA Compliance with Made in the US. We found lots of evidence that server production and manufacturing is outsourced to global companies like Foxconn and Flextronics and/or produced in countries like China, Mexico, Taiwan, India, Brazil, and Japan. There was some information in the public domain indicating that some suppliers produce storage and servers in factories in the US, but we could not determine if there were ordering options that would ensure country of origin (aside from the aforementioned availability of TAA compliant SKUs), or if their US manufacturing operations met the Made in the US criteria or were merely Assembled in the US. Our conclusion is that HPE appears to be the only large scale server manufacturer with an explicit option that ensures your industry standard server is Made in the US.

Cyber Catalyst Designation

Further demonstrating HPE’s commitment to cybersecurity of its products, The HPE Silicon Root of Trust and Aruba Policy Enforcement Firewall were among the 17 cybersecurity products and services designated out of 150+ applicants in the inaugural year of Cyber Catalyst by MarshSM program. Cyber Catalyst is Marsh's new cybersecurity evaluation program that enables customers that adopt designated technologies to be considered for enhanced terms and conditions on cyber insurance policies from participating insurers.1 Program applicants

---


cybersecurity-solutions-recognized-for-ability-to-reduce-risk-by-insurers-in-new-cyber-
catalyst-program.html, retrieved on September 26, 2020
How HPE is Leading Supply Chain Security
October, 2020

went through a two-stage evaluation consisting of a deep dive into eligible solutions that participating insurers feel merit the review, and then product and service demonstrations².

HPE is the first, and to-date, only manufacturer of industry standard servers to have the Cyber Catalyst designation on a key cybersecurity technology embedded in its servers. HPE Silicon Root of Trust can be found on HPE ProLiant servers, HPE Apollo systems, HPE Synergy Compute Modules, and HPE SimpliVity.

Penetration Testing

InfusionPoints has been HPE’s penetration testing security partner since 2017, and we’ve been invited to conduct numerous tests and analysis on HPE products and solutions. We’ve been impressed by HPE’s leadership in creating secure products, including the inclusion of independent, third party penetration testing and analysis. This testing goes deeper than the typical industry analyst style commissioned reports that we typically see from HPE’s competitors by subjecting HPE solutions to real-world modern threats and attack scenarios most likely to impact HPE customers.

Silicon Root of Trust and Server Recovery

InfusionPoints conducted two rounds of testing in the spring and fall of 2017 on HPE and its competitors. In the first round of testing, we compared features of the HPE Gen10 servers against three major competitors in the same class. In this test, HPE was the clear leader, providing a silicon root of trust anchored in the ILO chip, four cryptography options including FIPS and CNSA as well as other differentiators, including a class leading out-of-box security posture, chassis tamper detection that worked even when the server was unplugged, and run-time firmware integrity checks from the Silicon Root of Trust.

In the second round of testing, we really zeroed in on testing HPE’s silicon root of trust in the HPE Gen10 DL380 versus the root of trust in the also recently released Dell Gen14 R740 as well as the recovery capabilities of both. To conduct this test, we simulated a successful attack against the UEFI bios with the goal of injecting modifications to the bios image. This was done equally against both systems by leveraging physical means to introduce corruptions in each phase of the UEFI Platform Initialization process. We then observed to see how each system would respond.

The HPE Gen10 DL380 recovered from all 7 test scenarios while the Dell Gen14 R740 was able to recover from 5 of the 7 corruptions. The HPE Gen10 was usable during recovery, booting from an alternate firmware image, resulting in zero downtime. During the Dell R740 recovery process, the system was unresponsive for up to 15 minutes and would not allow the system to boot, leading us at first to believe that the system was bricked. InfusionPoints was able to demonstrate the HPE Gen10 server can recover its own iLO if its image becomes corrupt in some way. It was difficult to determine if Dell’s recovery technology provides recovery for the iDRAC.

When combined with HPE’s Server System Restore technology, customers get full stack protections from attacks including firmware, software, and data.

Conclusion

HPE continues to lead the market in security of its server hardware product lines. The addition of Made in the US supply chain options via the HPE Trusted Supply Chain initiative continues to demonstrate HPE’s commitment to developing secure products for its customers.

About InfusionPoints

InfusionPoints is your independent trusted partner dedicated to assisting you in building your secure and compliant business solutions, testing your security controls and defending your consumer, employee, and supply chain information.

Important Facts about this Paper

PUBLISHER: InfusionPoints, LLC

INQUIRIES: Contact us if you would like to discuss this report, and InfusionPoints will respond promptly.
+1-336-990-0252
info@InfusionPoints.com
https://www.infusionpoints.com

CITATIONS: This paper can be cited by accredited press and analysts but must be cited in-context, displaying author “InfusionPoints, LLC”. Non-press and non-analysts must request prior written permission by InfusionPoints, LLC for any citations.

LICENSING: This document, including any supporting materials, is owned by InfusionPoints, LLC. This publication may not be reproduced, distributed, or shared in any form without prior written permission from InfusionPoints, LLC.

DISCLOSURES: This paper was commissioned by Hewlett Packard Enterprise (HPE). InfusionPoints provides security research, analysis, advising, consulting, and penetration testing to many high tech companies in this space.

DISCLAIMER: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. InfusionPoints, LLC disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of InfusionPoints, LLC and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

InfusionPoints, LLC provides forecasts, and forward-looking statements, and trends in cybersecurity as directional indicators and not as precise predictions of future events. While our opinions are based on our current judgment based on available information and analysis, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinion as of the date of publication for this document.

Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

©2020 InfusionPoints, LLC. Company and product names are used for informational purposes only and may be trademarks of their respective owners.