



This Technical Advisory describes an issue which may or may not affect the customer's product

Intel Technical Advisory

TA-1148

5200 NE Elam Young Parkway
Hillsboro, OR 97124

September 13, 2019

Intel® Server System S9200WK Product Family firmware advisory

Products Affected

Product Name	Product Code
Intel® Server Systems	LWK2LC3UXXX01, LWK2LC3UXXX02, LWK2LC3UXXX03, LWK2LC3UXXX07, LWK2LC3UXXX05, LWK2LC3U5680A, LWK2LC3U4880A, LWK2AC3PXXX01
Intel® Server Compute Modules	S9248WK1HLC, S9256WK1HLCX, S9248WK1HLCX, S9248WK2HACX

Description

The IPMI Specification defines the host to Baseboard Management Controller (BMC) interface as a session-less interface where no authentication is required to issue IPMI commands to the BMC. The host-to-BMC interfaces are trusted, but not authenticated. If software executing on the host with user level privileges were to exploit a vulnerability resulting in a privilege escalation, the attacker would then be able to issue any IPMI commands to the BMC. This issue is associated with CVE-2019-11170.

Intel provides the option for customers to protect the BMC from the operating system by restricting or disabling the runtime Host IPMI interface to the BMC. Please note that this improved security mode may impact functionality of applications that utilize the KCS channel interfaces to communicate with the BMC.

KCS access is required for the host BIOS during the Pre-Boot phase. During this phase, BIOS communicates with the BMC for platform configurations through these channels. The default state for all systems is "Allow All". KCS commands can be accepted from BIOS/EFI without authentication. Alerts on the EWS page and/or security sensors, can transition to "Restricted" or "Deny All" with IPMI commands from any interface. Customers must decide which KCS policy ("Allow All", "Deny All", or "Restricted") is best suited for their environment.

Root Cause

The IPMI Specification definition for the local host to BMC interface.

Corrective Action / Resolution

This issue is resolved in Baseboard Management Controller firmware to release v2.18 and later. Intel recommends updating the BMC firmware at the earliest opportunity.

As part of the mitigation of this issue, new KCS control policies will be implemented in the Baseboard Management Controller's firmware. The new KCS policies implement new policies of "Allow All", "Deny All", and "Restricted". These new policies are described in BMC Firmware External Product Specification (EPS) v1.18. Intel strongly recommends that customers read and understand the new control policies prior to configuring and setting up their server management network. This BMC firmware EPS may be downloaded from the Intel Support website at <https://cdrdv2.intel.com/v1/dl/getContent/598340>.

Recommended Customer Action

Customers of products listed in the affected products table should update their server systems immediately to mitigate this issue. For additional information or questions concerning this advisory, please contact your Intel® Customer Support representative. When contacting the Intel® Customer Support representative about this advisory, please mention this Technical Advisory.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel Corporation