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

Intel Technical Advisory

TA-1155

5200 NE Elam Young Parkway
Hillsboro, OR 97124

June 4, 2020

Baseboard Management Controller (BMC) Keyboard Controller Style (KCS) Interface Advisory

Products Affected

Product Type	Product Name	MM#
Intel® Server Board	S2600WT2R	943786
	S2600WTTR	943785
	S2600WTTS1R	949339
	DBS2600CW2R	943803
	DBS2600CWTR	943805
	DBS2600CW2SR	943804
	DBS2600CWTSR	943806
	S2600KPR	943789
	S2600KPFR	943790
	S2600KPTR	948036
	S2600TPR	943944
	S2600TPFR	943947
	S2600TPTR	953032
	S2600TPNR	955259
	DBS1200SPL	944682
	DBS1200SPS	944683
	DBS1200SPO	944684
Intel® Compute Module	HNS2600KPR	943787
	HNS2600KPFR	943788
	HNS2600TPR	943948
	HNS2600TPFR	943949
	HNS2600TPNR	955260
	HNS2600TP24R	943951
	HNS2600TP24SR	945609
	HNS2600TP24STR	953190
Intel® Server System	R1304WTTGSR	943891
	R1304WT2GSR	943892
	R1208WTTGSR	943893
	R1208WT2GSR	943894
	R2208WT2YSR	943827
	R2208WTTYSR	943826
	R2208WTTYC1R	943828
	R2308WTTYSR	943829

R2312WTTYSR	943830
R2224WTTYSR	943831
R1304SPOSHBN	944471
R1304SPOSHOR	944476
R1208SPOSHOR	944477

Description
The Intelligent Platform Management Interface (IPMI) Specification defines the host to 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 Embedded Web Server (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
For Intel Server Board S2600WT, S2600CW, S2600TP and S2600KP family boards this issue is resolved in Baseboard Management Controller firmware of release v1.61 and later.
For Intel Server Board S1200SP Product Family this issue is resolved in Baseboard Management Controller firmware of release v1.19 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). For Intel Server Board S2600WT, S2600CW, S2600TP and S2600KP family boards please refer to BMC EPS v1.20 and for Intel Server Board S1200SP Product Family please refer to BMC EPS v1.2.
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:
Intel Server Board S2600WT, S2600CW, S2600TP and S2600KP family boards BMC EPS v1.20 at {https://cdrdv2.intel.com/v1/dl/getContent/573094}.
Intel Server Board S1200SP Product Family BMC EPS v1.2 at {https://cdrdv2.intel.com/v1/dl/getContent/619577}.

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.

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