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

Intel Technical Advisory

TA-1143

5200 NE Elam Young Parkway
Hillsboro, OR 97124

Jan 25, 2019

Invocation of the ipmitool from the remote system requires extra parameters to connect to Intel® Server systems that have BMC firmware v1.90 or later installed.

Affected Products

Product Type	Product Name	MM#
Intel® Server Board	BBS2600BPB	948899
	BBS2600BPQ	948900
	BBS2600BPS	952609
	BBS2600BPBR	986113
	BBS2600BPQR	986115
	BBS2600BPSR	986114
	S2600WF0	952644
	S2600WFQ	952645
	S2600WFT	952641
	S2600WF0R	986005
	S2600WFQR	986006
	S2600WFTR	986004
	S2600STB	957180
	S2600STQ	957318
	S2600STBR	986246
	S2600STQR	986307
	BBS2600STB	959820
	BBS2600STQ	959727
	BBS2600STBR	986308

	BBS2600STQR	986309
Intel® Compute Module	HNS2600BPB	976668
	HNS2600BPQ	976669
	HNS2600BPS	976670
	HNS2600BPB24	976671
	HNS2600BPQ24	976675
	HNS2600BPS24	976676
	HNS2600BPBLC	961401
	HNS2600BPBLC24	977207
	HNS2600BPBR	986116
	HNS2600BPBRX	986123
	HPCHNS2600BPBR	999DAM
	HNS2600BPQR	985900
	HPCHNS2600BPQR	999DAP
	HNS2600BPSR	986117
	HPCHNS2600BPSR	999DAN
	HNS2600BPB24R	986118
	HNS2600BPB24RX	986124
	HNS2600BPQ24R	986120
	HNS2600BPS24R	986119
	HNS2600BPBLCR	986121
	HNS2600BPBLC24R	986122
Intel® Server System	R1304WF0YS	952626
	R1304WFTYS	952625
	R1208WFTYS	952627
	R2308WFTZS	952631
	R2208WF0ZS	952629
	R2208WFTZS	952628
	R2208WFQZS	952637
	R2312WF0NP	955876
	R2312WFTZS	952632
	R2312WFQZS	955877
	R2224WFQZS	955875
	R2224WFTZS	952633
	R1208WFTYSR	986007

	HPCR1208WFTYSR	999AKZ
	R1304WF0YSR	986047
	HPCR1304WF0YSR	999AL0
	R1304WFTYSR	986048
	HPCR1304WFTYSR	999AL1
	R2208WFTZSR	986049
	R2208WFTZSRX	9999P2
	HPCR2208WFTZSR	999AL2
	HPCR2208WFTZSRX	999CKN
	R2208WF0ZSR	986050
	HPCR2208WF0ZSR	999ALC
	R2224WFTZSR	986051
	HPCR2224WFTZSR	999AM0
	R2308WFTZSR	986052
	HPCR2308WFTZSR	999AM1
	R2312WFTZSR	986053
	HPCR2312WFTZSR	999AM2
	R2312WF0NPR	986054
	HPCR2312WF0NPR	999AM3
	R2208WFQZSR	986055
	HPCR2208WFQZSR	999AM4
	R1208WFQYSR	986059
	HPCR1208WFQYSR	999AM8

Description

Beginning with BMC firmware version 1.90, invocation of the ipmitool from a remote system requires the following extra parameter: "`-C 17`". This parameter is required due to the BMC disabling Cipher Suite 3 by default, leaving only Cipher Suite 17 enabled by default.

Note: Unrelated to this change, it has been observed in networks with high traffic loads that ipmitool commands may trigger a default timeout setting (1 second). Intel® recommends that customers experiencing timeouts also add the parameter "`-N 5`" (setting the timeout to 5 seconds) to the required "`-C 17`".

With both required and recommended additions to the remote ipmitool invocation, the command line syntax is as follows (type on a single command line):

```
# ipmitool -I lanplus -H ip.ad.dr.ess -U user -P password -C 17 -N 5 command <options>
```

Root Cause

Cipher Suite 17 and 3 are the only cipher suites that implement any level of secure confidentiality algorithm. However, due to documentation of both hmac-md5 and md5 integrity algorithms being inherently weak, they should be used neither for integrity nor for authentication.

To enhance BMC firmware security beginning with BMC firmware revision 1.90, Intel has disabled Cipher Suite 3 by default, leaving only Cipher Suite 17 enabled by default. As a result, ipmitool use from remote consoles must force utilization of Cipher Suite 17 by adding "`-C 17`" to the command line to connect to Intel® Server systems having BMC firmware revision 1.90 or later installed.

Cipher Suite 17 support was introduced in ipmitool release 1.8.18 on October 8th 2016, and is the minimum version required that can be used to connect to Intel® Server systems having BMC firmware revision 1.90 or later installed.

Intel has submitted code to the ipmitool community to automatically rank cipher suite desirability/security as follows: 17 > 3 >> all the rest, at:

https://github.com/ipmitool/ipmitool/commit/7772254b62826b894ca629df8c597030a98f4f72

The latest source version of ipmitool includes an automatic attempt to use the most secure supported version of Cipher Suite. This update ensures that -C is not needed after a new binary release of ipmitool including this code is made available in the future. Customers can download the source from the latest version at:

https://github.com/ipmitool/ipmitool

Users can then recompile ipmitool by themselves to take advantage of this improvement before an official release is made by the ipmitool community.

Workaround

If customer requires use of Cipher Suite 3 in addition to Cipher Suite 17, the below commands may be used (grouped by local host / remote console, and then by connected network port, and finally by ipmitool lan command / ipmitool raw command), also the Cipher Suite 3 can be enabled from the embedded web console.

From local host:

```
## Shared NIC 1

# ipmitool lan set 1 cipher_privs XXaXXXXXXXaXXXX

## Shared NIC 2

# ipmitool lan set 2 cipher_privs XXaXXXXXXXaXXXX

## Dedicated Management NIC

# ipmitool lan set 3 cipher_privs XXaXXXXXXXaXXXX
```

or

```
## Shared NIC 1

# ipmitool raw 0x0c 0x01 0x01 0x18 0x00 0x00 0x04 0x00 0x00 0x00 0x04 0x00
0x00

## Shared NIC 2

# ipmitool raw 0x0c 0x01 0x02 0x18 0x00 0x00 0x04 0x00 0x00 0x00 0x04 0x00
0x00

## Dedicated Management NIC

# ipmitool raw 0x0c 0x01 0x03 0x18 0x00 0x00 0x04 0x00 0x00 0x00 0x04 0x00
0x00
```

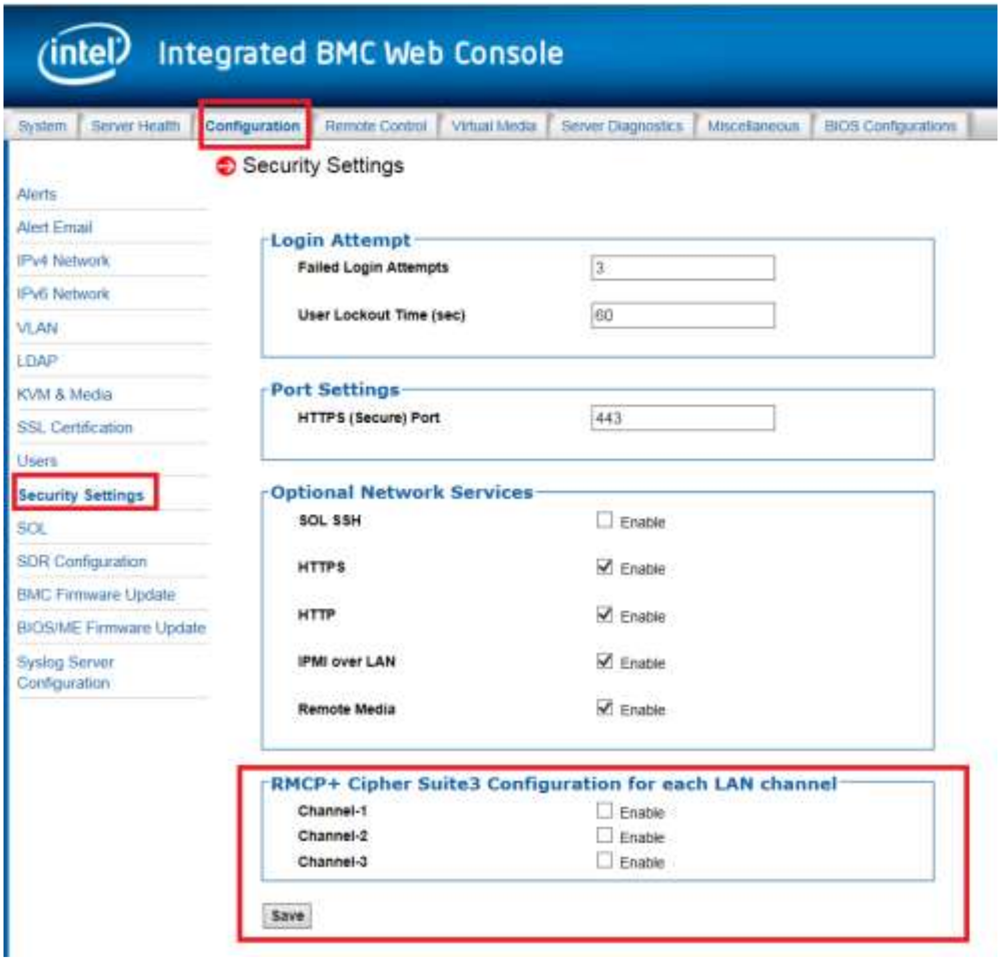
From a remote client:

```
## Shared NIC 1 (type the following on a single line)

# ipmitool -I lanplus -H ip -U user -P password lan set 1 cipher_privs XXaXXXXXXXaXXXX

## Shared NIC 2 (type the following on a single line)

# ipmitool -I lanplus -H ip -U user -P password lan set 2 cipher_privs XXaXXXXXXXaXXXX

## Dedicated Management NIC (type the following on a single line)

# ipmitool -I lanplus -H ip -U user -P password lan set 3 cipher_privs XXaXXXXXXXaXXXX
```

or

```
## Shared NIC 1 (type the following on a single line)

# ipmitool -I lanplus -H IP -U user -P password raw 0x0c 0x01 0x01 0x18 0x00 0x00 0x04 0x00
0x00 0x00 0x04 0x00 0x00

## Shared NIC 2 (type the following on a single line)

# ipmitool -I lanplus -H IP -U user -P password raw 0x0c 0x01 0x02 0x18 0x00 0x00 0x04 0x00
0x00 0x00 0x04 0x00 0x00

## Dedicated Management NIC (type the following on a single line)

# ipmitool -I lanplus -H IP -U user -P password raw 0x0c 0x01 0x03 0x18 0x00 0x00 0x04 0x00
0x00 0x00 0x04 0x00 0x00
```

Or enable Cipher Suite 3 from the embedded web console (Configuration-->Security Settings--> RMCP+ Cipher Suite 3 configuration)



Security Settings

Login Attempt

Failed Login Attempts: 3

User Lockout Time (sec): 60

Port Settings

HTTPS (Secure) Port: 443

Optional Network Services

SOL SSH □ Enable

HTTPS ☑ Enable

HTTP ☑ Enable

IPMI over LAN ☑ Enable

Remote Media ☑ Enable

RMCP+ Cipher Suite3 Configuration for each LAN channel

Channel-1 □ Enable

Channel-2 □ Enable

Channel-3 □ Enable

Please contact your Intel Sales Representative if you require more specific information about this issue.

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.