*This technical advisory describes an issue, which may or may not affect the customer's product.*

# Intel Technical Advisory

**TA-1176-01**

5200 NE Elam Young Parkway
Hillsboro, OR 97124

March 08, 2022

## BMC SSL certificate and private key loaded on the system may be replaced when upgrading BMC firmware to version 2.86.2da97d3f

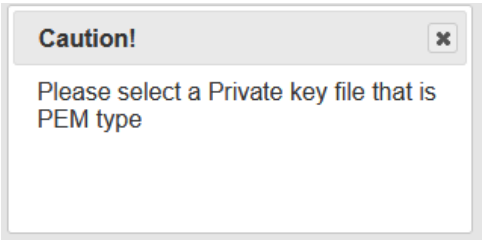
### Products Affected

| Product Name | Product Code |
|---|---|
| **Intel® Server Systems** | Intel® Server Systems R1000WFR Family<br>Intel® Server Systems R2000WFR Family<br>Intel® Server System S9200WK Family<br>Intel® Server System M20MYP Family |
| **Intel® Server Compute Modules** | Intel® Compute Module HNS2600BP Family |
| **Intel® Server Boards** | Intel® Server Board S2600BPR Family<br>Intel® Server Board S2600WFR Family<br>Intel® Server Board S2600STR Family |

### Description

When upgrading the system's baseboard management controller (BMC) firmware to version 2.86.2da97d3f, the BMC SSL certificate and the private key may be replaced by an Intel self-signed certificate if the previous loaded certificate uses a private key from a file with `.key` extension. In this case, the BMC reboot cycle takes longer and the event entry is logged into the system event log (SEL) as "Reserved SSL Certificates reset – Asserted".

Additionally, in the BMC version 2.86.2da97d3f, when trying to upload a private key file with the extension `.key` via **Integrated BMC EWS > New Private Key** option **> Choose File** button, a caution pop-up window is displayed with the message: "Please select a Private key file that is PEM type" (see the following figure).




### Root Cause

The BMC firmware version 2.86.2da97d3f is implementing validation of the file content and extension when loading the BMC SSL certificate and private key. This measure is taken to improve the system protection against malicious software and malware attacks. As a result, only `.pem` files are accepted to be loaded as private key.

After updating the system to the BMC firmware version 2.86.2da97d3f, the system reboots and checks for the format of the private key file. If the existing private key file has a `.key` extension, the certificate and private key are replaced with an Intel self-signed certificate to ensure that the Integrated BMC Embedded Web Server (EWS) can be accessed successfully. The event is logged in the SEL as "Reserved SSL Certificates reset – Asserted".

**Corrective Action / Resolution**

If the customer is using a private key with `.key` extension, the private key must be replaced with a `.pem` file before upgrading the BMC firmware to version 2.86.2da97d3f.

If the customer's certificate has been replaced by the Intel self-signed certificate in the Integrated BMC EWS, the customer can load a new BMC SSL certificate by using a private key with `.pem` extension.

Please note that there is no impact if the customer is using the Integrated BMC EWS' Intel self-signed certificate, or is using a chained-certificate private key with a `.pem` format.

Refer to the *Integrated Baseboard Management Controller Embedded Web Server User Guide* for Intel® server systems for instructions on how to upload a new SSL certificate and private key.

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 and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.