

#### Infineon TPM Security Update

Release date : Nov 6, 2017 Last update : JAN 16, 2023 Potential Security Impact: Potential loss of confidentiality Source: Infineon

Overview

A security vulnerability was identified in the RSA key generation method used by TPM products listed below. This leaves the keys potentially vulnerable via targeted, computationally expensive attacks. These RSA keys generated by the TPM are used with certain software products and should not be considered secure. Updated TPM firmware versions which enable more secure key generation are listed in the RESOLUTION section for the following dedicated TPM products.

• SLB 9665 (TPM 2.0)

#### NOTE:

SLB 9635 (TPM 1.2) is not affected. Reference Number CVE-2017-15361

### Impacted Products

Getac has provided the following updates for Infineon Trusted Platform Module. For details on the impact of this firmware update for Windows software such as BitLocker see the following Microsoft advisory:<u>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV170012</u>.

		TPM (Infineon)		
Product	CPU Generation	The previous	The latest	
name		version of	update	Customer download link
		TPM FW	<b>TPM FW</b>	
V110	6th Gen Core	V5.51	V5.62	
F110	6th Gen Core	V5.51	V5.62	
S410	6th Gen Core	V5.51	V5.62	https://support.getac.com/Service/FileReader
B300	6th Gen Core	V5.51	V5.62	/Index?fileid=108709&cateid=100043
RX10	5th Gen Core	V5.51	V5.62	
Т800	CHT T4	V5.51	V5.62	

# **Getac** How to check TPM Firmware version

1. Open "Command Prompt"



2. Key in "tpm.msc" and press "Enter" key, then "Trusted Platform Module (TPM) Management on Local Computer" window will be popped up.

Command Prompt	-	×	
RecyMicrosoft Windows [Version 10.0.18363.959] (c) 2019 Microsoft Corporation. All rights reserved.		^	
C:\Users\Getac123>tpm.msc_			
G-M.			

3. Check Manufacturer version on TPM Manufacturer information.

Command Prompt Command Prompt	Management on Local Computer Help	- C X
C: Ulsers\Getac123> GM. C: Ulsers\Getac123> C: Ulsers\Getac123 C: Ulsers\Getac123 C: Ulsers\Getac123 C: Ul	TPM Management on Local Computer  TPM Management on Local Computer  Configures the TPM and its support by the Windows platform  Overview  Windows computers containing a Trusted Platform Module (TPM) provide enhanced security features. This support of the plays information about the computer's TPM and allows administrators to manage the device.  Status  The TPM is mady for use.  Available Options  You may clear the TPM to remove ownership and reset the TPM to factory defaults.  TPM Manufacturer Information  Manufacturer Information  Manufacturer Name.  Available Options  Avail	Actions TPM Management on Local Computer A Prepare the TPM Clear TPM View New Window from Here Refresh Help
Type here to search		∧ 11:21 PM 1(12) PM

4. Please apply below TPM firmware update steps if TPM version is lower than V5.62.

# **Getac** How to Update TPM Firmware

## **Applications**

The TPM firmware update is applicable to the following models.

Model Name	System Release
RX10	MP model
F110G3	MP model
V110G3	MP model
B300G6	MP model
S410	MP model
T800G2	MP model

## **Update Procedures**

## Part 1. Create a USB drive for the firmware update.

- 5. Insert a USB drive.
- 6. Format the USB drive to FAT32. (The original data on the USB drive will be erased.)
- 7. Download the TPMFWUpd.zip file from

https://support.getac.com/Service/FileReader/Index?fileid=108709&cateid=100043

8. Decompress the **TPMFWUpd.zip** file to the USB drive. The below screen shows the result.

US	USBDISK (D:) V 🗘 Sea		Search USBDIS	K (D:)
^	Name	Date modified	Туре	Size
	EFI	11/22/2017 9:20 A	File folder	
	IFXTPMUpdate.efi	11/15/2017 3:46 PM	EFI File	288 KB
	Readme	11/22/2017 11:33	Text Document	1 KB
	TPM20_5_62_3126_0.BIN	7/20/2017 5:20 PM	BIN File	351 KB
	TPMUpd.efi	11/22/2017 11:43	EFI File	24 KB
	Update.nsh	11/22/2017 11:15	NSH File	1 KB

9. Remove the USB drive.



## Part 2. Update the TPM firmware.

**NOTE:** TPM firmware update will cause loss of all TPM keys and data protected by those keys.

1. Disable **BitLocker** on Windows OS (Windows 7 Enterprise/Ultimate and Windows 10). Select **Control Panel** → **System and Security**→ **BitLocker Drive Encryption**. Turn off **BitLocker**.

Home	BitLocker Drive Encryption			
	Help protect your files and folders from unaut	horized acces	s by p	protecting y
	Operating system drive			
	Operating system drive Windows (C:) BitLocker off			

- 2. Restart the system.
- 3. Enter SCU (BIOS Setup Utility) by pressing **F2** during POST. (See the *User Manual* of your product to know alternative ways to enter SCU.)
- 4. Select **Security** to open the Security menu.
- 5. Select the TPM Setup Menu item. Change TPM Support from [Enabled] to [Disabled].
- 6. Go back to the Security menu.
- 7. Change Intel Trusted Execution Technology from [Enabled] to [Disabled].
- 8. Save and exit SCU.
- 9. Insert the USB drive you created previously.
- 10. Restart the system.
- 11. Enter Boot Manager.
  - For notebook models, press F10 during POST.
  - For tablet models, press the **Menu** hardware button or tap the touchscreen during POST.



12. Select EFI USB Device and press Enter. (On tablet models, the Enter key is the Windows logo Hardware button.) This allows EFI boot from the USB drive containing the TPM firmware update.

Boot Manager
Boot Option Menu EFI Boot Devices Windows Boot Manager (PLEXTOR PX-25667LeV) EFI USB Device (JetFlashTranscend 16GB) EFI Network 0 for IPv4 (00-22-20-15-ED-38) EFI Network 0 for IPv6 (00-22-20-15-ED-38) 1 and 4 to change option, ENTER to select an option, ESC to exit

13. Press any key to continue.

Execute TPM 2.0 firmware update to 5.62 WARNING TPM FW update cause lose all TPM keys and data protected by those keys. Please mak sure bitlocker function was off state. Do you want to continue update TPM firmware ? Enter 'q' to quit, any other key to continue:

- 14. Wait for the TPM firmware update and TPM provision to complete.
- 15. When completed, press the power button to turn off the system.
- 16. Turn on the system.
- 17. Enter SCU (BIOS Setup Utility).
- 18. Select Security to open the Security menu.

Select the TPM Setup Menu item. Change TPM Support from [Disabled] to [Enabled].

### **Getac Disclaimer:**

All content and other information mentioned in this statement or offered arising from the issue described herein are provided on an "as is" basis. Getac hereby expressly disclaims any warranties of any kind, express or implied, including without limitation warranties of merchantability, fitness for any particular purpose, non-infringement of intellectual property. All products, information, and figures specified are preliminary based on current expectations and Getac reserves the right to change or update any content thereof at any time without prior notice. Getac assessments have been estimated or simulated using Getac internal analysis or architecture simulation or modeling, and may not represent the actual risk to the users' local installation and individual



environment. Users are recommended to determine the applicability of this statement to their specified environments and take appropriate actions. The use of this statement, and all consequences of such use, is solely at the user's own responsibility, risk, and expense thereof. In no event shall Getac or any of its affiliates be liable for any and all claims, damages, costs or expenses, including without limitation, loss of profits, loss of data, loss of business expectancy, compensatory, direct, indirect, consequential, punitive, special, or incidental damages or business interruption arising out of or in connection with related to the information contained herein or actions that the user decides to take based thereon. Getac reserves the right to interpret this disclaimer and update this disclaimer whenever necessary.