

TSB 3039-00

TPM UPDATE PROCEDURE

TSB 3039-00 - TPM ADVISORY AND UPDATE

This update is provided by Razer to address the TPM security advisory published by Microsoft® and Infineon®. For more details regarding these announcements please scroll to the appendix at the bottom of this document.

Razer Blade Models affected by this update:

Model Number	Description
RZ09-1652	Razer Blade 14" (2016) GTX970M
RZ09-1952	Razer Blade 14" (2016) Intel 6700HQ GTX1060
RZ09-1953	Razer Blade 14" (2017) Intel 7700HQ GTX1060
RZ09-01682	Razer Blade Stealth 12.5" (2016) Intel 6500U
RZ09-01962	Razer Blade Stealth 12.5" (2016) Intel 7500U
RZ09-01662	Razer Blade 17" (2016)
RZ09-01663	Razer Blade 17" (2017)

If your Razer Blade is not listed above, please do not run the TPM Updater in your system.
If your Razer Blades is listed above, please proceed reading this article.

Before you start:

a) Please ensure you have installed all the latest Microsoft® Windows Operating Systems and Security Updates.

For help verifying your OS is up to date, please refer to the following Microsoft® article:

https://support.microsoft.com/en-us/help/4027667/windows-update-windows-10

b) Ensure your Blade is plugged into a wall outlet and not running on battery alone before proceeding.

TPM Updater – Step-by-Step Process

IMPORTANT: To run the TPM Updater, you will need to go to your Razer Blade BIOS Utility and temporally disable the current TPM platform. You will also need re-enable it once you are done running the TPM Updater. By default, Razer Blade's TPM is enabled in your Bios Utility – in case you may have disabled it on your own beforehand, you may skip Step 1.

Please Note - The TPM Updater will not allow you to continue until TPM is disabled in the BIOS Utility.

Step 1: Disable the TPM Updater in your Razer Blade Bios Utility

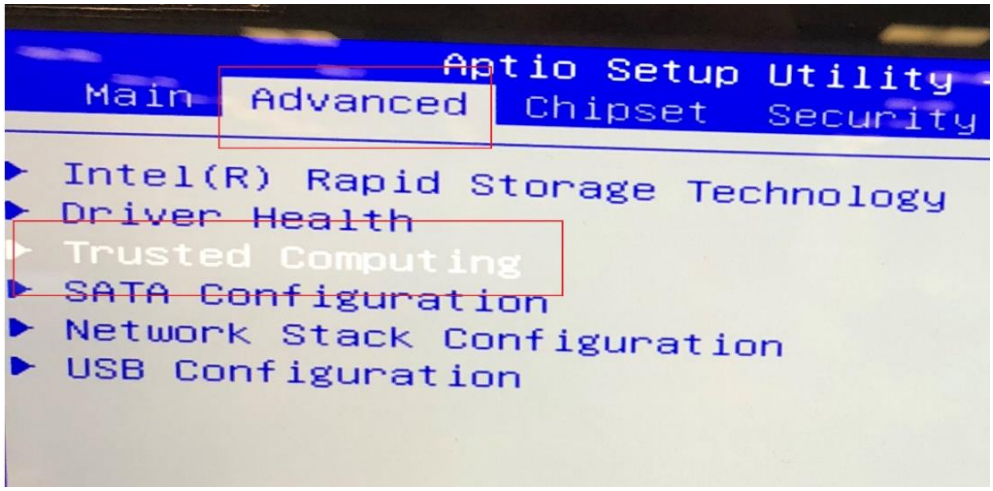
a) Restart the laptop

b) At restart, once the "Razer Logo" appears on the screen, tap the F1 key repeatedly

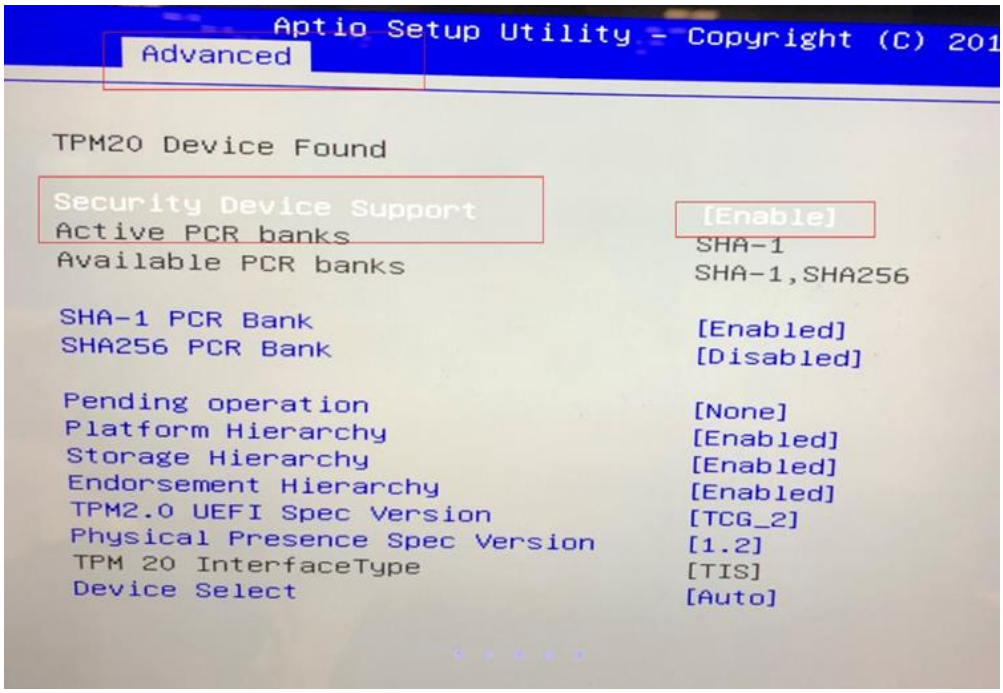
c) The BIOS Utility will launch

d) From the Main BIOS screen, go to the "Advanced" Tab

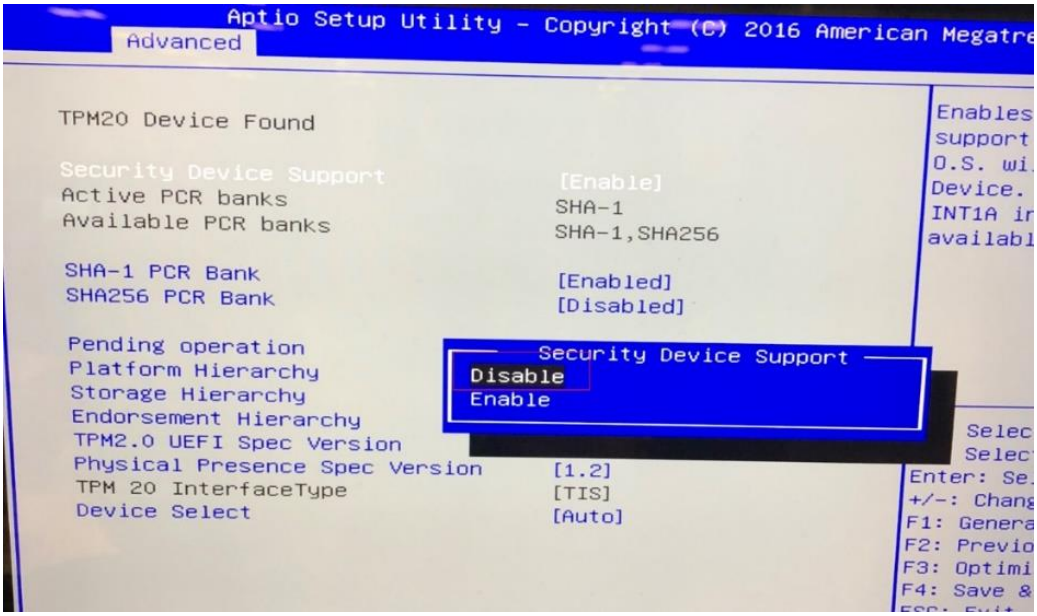
e) Select "Trusted Computing" as shown below:



f) Under “Trusted Computing”, select “Security Device Support”, as shown below:

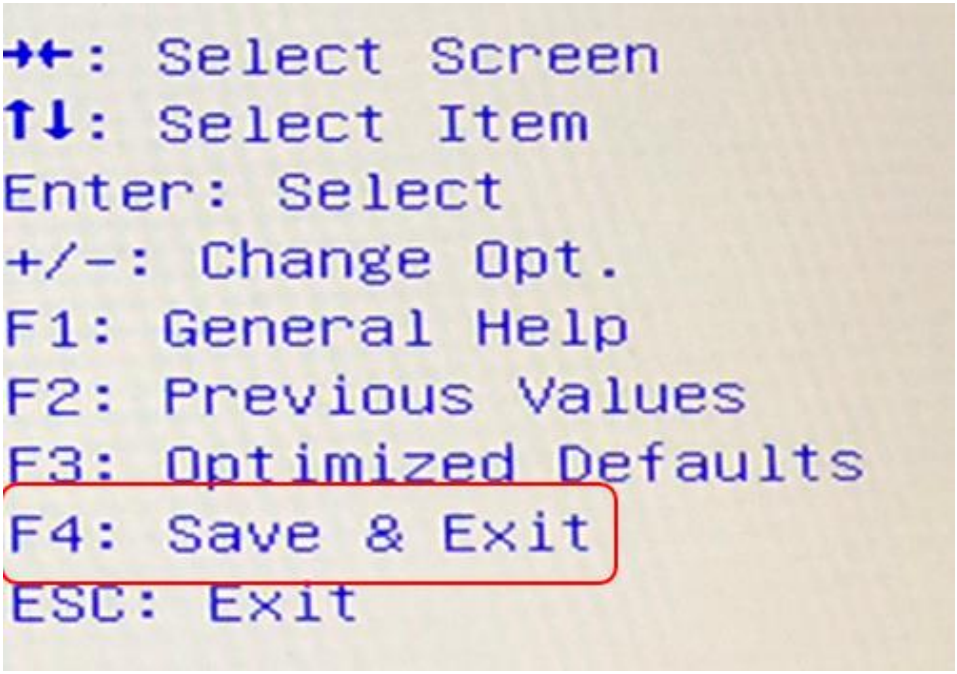


g) Under **“Security Device Support”** press the enter key once, select **"Disable"** and press the enter key again to confirm:



h) Once successfully disabled, **"Security Device Support"** should now show **"Disable"**

i) Press the F4 key to save and Exit



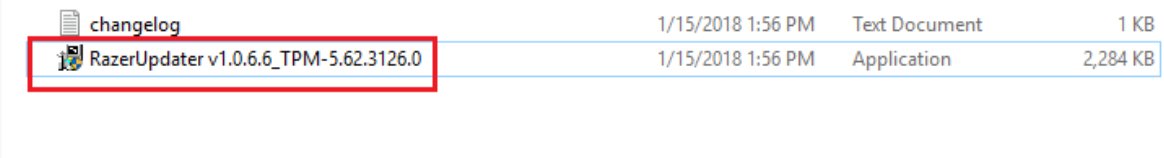
j) The System should automatically restart

k) Now that the TPM has been disabled, your system is ready to run the TPM Updater

Step 2: Downloading, extracting and installing the TPM Utility

a) Click on the link below, download and save the TPM Updater into your system
http://drivers.razersupport.com//index.php?_m=downloads&_a=viewdownload&downloaditemid=2765&nav=0,350,604,605

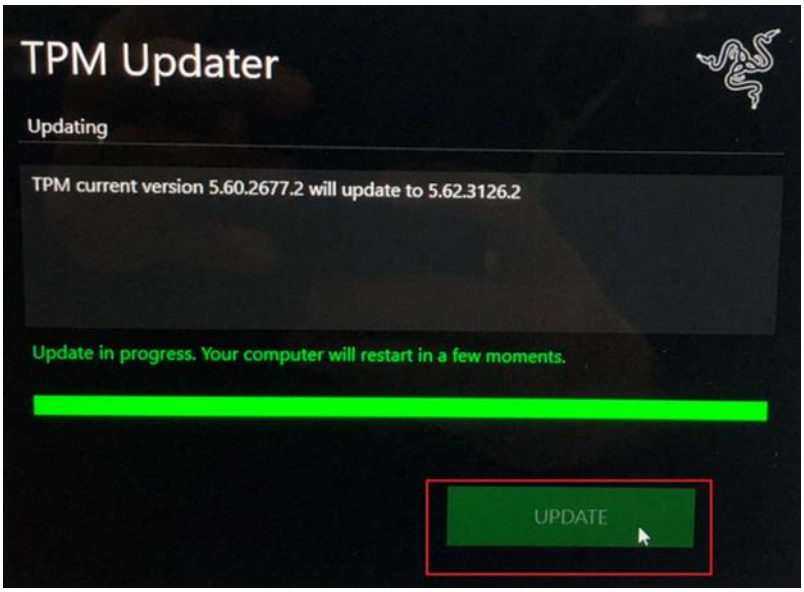
b) Double click on the downloaded file to extract and run the TPM Updater.



c) The TPM Updater will launch and will display the current version of the TPM and the version it will update to.

d) Click on the “Update” button to proceed

e) The green bar will show you the status as the system gets updated, as shown below:

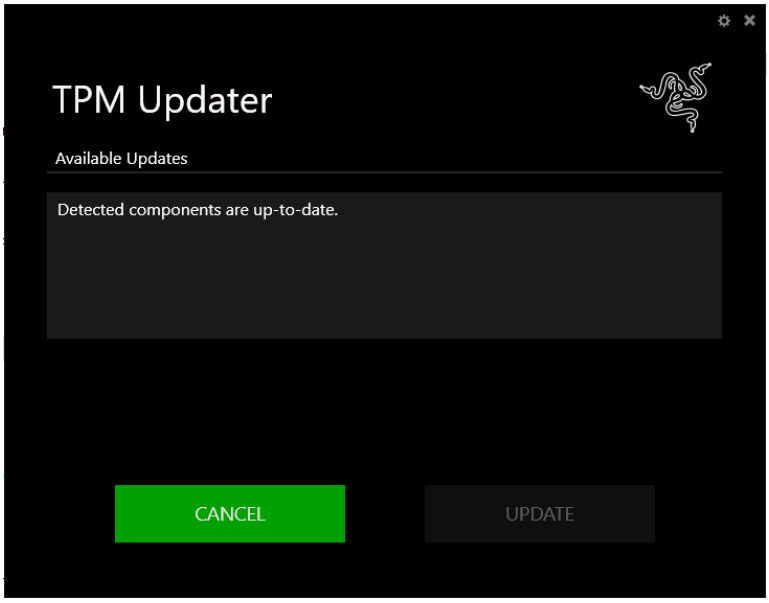


f) The System should automatically restart.

g) Log in back into your system and run the TPM Updater tool again



h) The TPM Updater will launch and you should see the prompt below indicating the successful update, as shown below:



Step 3: Re-enable TPM in the BIOS

Now that your system has been updated, be sure to go back to your Razer Blade Bios Utility and re-enable TPM, failure to do so may put your computer at risk.

a) Please refer and repeat Step 1 in this document - but this time, change “Security Device Support" back from "Disabled" to "Enabled"

b) Be sure to select “Save and Exit” to save these changes

Step 4: End

Appendix

NOTE: This update is applicable to systems using Infineon TPM chip with firmware 5.0.1089.2, 5.60.2677.0, 5.60.2677.2, 5.61.2785.0, 5.61.2785.2

Potential Security Impact:
Microsoft® Security Advisory ADV170012 addresses a security vulnerability issue in certain TPM on Infineon® main boards. This vulnerability is in the TPM chip itself, and not in Windows and it leaves the RSA keys generated by the Infineon TPM using certain firmware levels rather insecure by making it easier for attackers to defeat various cryptographic protection mechanisms via targeted attacks.
Note: Only software that uses RSA keys generated by the TPM is affected by this vulnerability.

* **Source:** Infineon® & Microsoft® Security announcement & updates
- **Microsoft**
- **Infineon**

Razer is aware of public announcements and discussions of the above referred security vulnerability.

The Razer team has worked with its required partners to investigate, validate, and test this security vulnerability. There is a small list of Razer's products affected as noted above.

The Trusted Platform Module (TPM) is a microcontroller on the system board used to securely store artifacts used to authenticate the platform, such as passwords, certificates or encryption keys, or measurements to ensure your system is trustworthy.

For more detailed information please refer to the Infineon web site:

http://www.infineon.com/TPM-update

Microsoft has published additional information relating to operating systems.For detailed information please refer to the Microsoft web site:

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170012

NATIONAL VULNERABILITY DATABASE

https://nvd.nist.gov/vuln/detail/CVE-2017-15361