Infineon TPM Vulnerability
List of affected OEM Mainboards

On their web page (October 10, 2017), Infineon published security information about a research team developed advanced mathematical methods to analyze and exploit weaknesses in acceleration algorithms for prime number finding, which are common practice today for RSA key generation.

Dezember 21, 2017

Affected OEM Mainboards	New Mainboard Revision with updated TPM (FW V5.62) from 01/2018	Used TPM Version	Fixed with TPM Update Tool (Field Update)
D3243-S1	--	Infineon SLB9660 TT1.2 FW4.40	Tool 1
D3313-Sx (with opt. TPM 1.2 Module only)	--	Infineon SLB9660 TT1.2 FW4.40	Tool 1
D3348-B1	--	Infineon SLB9660 TT1.2 FW4.40	Tool 1
D3348-B2	**X**	Infineon SLB9665 TT2.0 FW5.51	tbd
D3402-B1 (GS1/GS2)	--	Infineon SLB9665 TT2.0 FW5.50	Tool 2
D3402-B1 (GS3)	--	Infineon SLB9665 TT2.0 FW5.51	Tool 2
D3402-B2	**X**	Infineon SLB9665 TT2.0 FW5.60	Tool 2
D3417-B1 (GS1/GS2)	--	Infineon SLB9665 TT2.0 FW5.50	Tool 2
D3417-B1 (GS3)	--	Infineon SLB9665 TT2.0 FW5.51	Tool 2
D3417-B2	**X**	Infineon SLB9665 TT2.0 FW5.60	Tool 2
D3433-S1	--	Infineon SLB9665 TT2.0 FW5.51	Tool 2 [1)]
D3433-S2	**X**	Infineon SLB9665 TT2.0 FW5.61	Tool 2
D3441-S1	--	Infineon SLB9665 TT2.0 FW5.51	Tool 2 [1)]
D3441-S2	**X**	Infineon SLB9665 TT2.0 FW5.61	Tool 2
D3446-S1	**X**	Infineon SLB9665 TT2.0 FW5.51	Tool 2 [1)]
D3446-S2	**X**	Infineon SLB9665 TT2.0 FW5.61	Tool 2

1) Updated BIOS ≥ R1.21.0 required (available from cw03/2018)

■ Fujitsu recommends to update the BIOS to the latest released version before applying a TPM firmware update.

Published by department
Systemboard OEM Sales

Oem-marketing@ts.fujitsu.com

http://www.fujitsu.com/fts/products/computing/pc/accessories/mainboards/

OEM FTP
ftp://ftp.ts.fujitsu.com/pub/Mainboard-OEM-Sales/