Intel® Converged Security Management Engine (Intel® CSME) Q2'2018 Security Release

&

Power Management Controller (PMC) Security Vulnerability in Systems using specific Intel® Converged Security and Management Engine (CSME) or Intel® Server Platform Services firmware versions

List of affected Fujitsu Products

Potential Exposure of Intel CSME assets through physical access (CVE-2018-3655, INTEL-SA-00125)
A Release of upgrades for Intel Active Management Technology (CVE-2018-3657, CVE-2018-3658, CVE-2018-3616, INTEL-SA-00141)
Intel® AMT 9.x/10.x/11.x/12.0 ROBOT TLS (CVE-2018-3616, INTEL-SA-00141)
Firmware updates for Intel® Platform Trust Technology (Intel® PTT) security vulnerabilities (CVE-2018-3659, INTEL-SA-00142)
Power Management controller (PMC) Security Vulnerabilities in Systems using specific Intel® CSME or Intel® Server Platform Services Firmware versions (CVE-2018-3643, INTEL-SA-00131)

We continue to urge all customers to keep their systems up-to-date.

Last update:
December 11, 2019

Notes
- This is an overview of affected Fujitsu products.
- This list is updated regularly (affected products, dates and BIOS versions).
- For the supply of an updated BIOS we rely on the support of the component supplier.
  Further we only can provide fixes for products which are under service.
  Products which are not listed below are either not affected or out of services.

OEM Mainboard

	CVE-2018-3655,-3657, -3658,-3659		CVE-2018-3616	
Affected Mainboard	New BIOS (with fix)	BIOS release date	New BIOS (with fix)	BIOS release date
D3220-B	---	---	R1.46.0	available
D3221-B	---	---	R1.46.0	available
D3222-B	---	---	R1.46.0	available
D3230-B	---	---	R1.46.0	available
D3231-S1	---	---	yes	t.b.d.
D3235-S1	---	---	yes	t.b.d.
D3236-K	---	---	yes	t.b.d.
D3236-R	---	---	yes	t.b.d.
D3236-S1	---	---	yes	t.b.d.
D3240-B1	---	---	R1.46.0	available
D3243-S1	---	---	yes	t.b.d.
D3400-B1	R1.27.0	available	R1.27.0	available
D3400-B2	R1.19.0	available	R1.19.0	available
D3401-B1	R1.27.0	available	R1.27.0	available
D3401-B2	R1.19.0	available	R1.19.0	available
D3402-B1	R1.27.0	available	R1.27.0	available
D3402-B2	R1.19.0	available	R1.19.0	available
D3410-B1	R1.27.0	available	R1.27.0	available
D3410-B2	R1.19.0	available	R1.19.0	available
D3417-B1	R1.27.0	available	R1.27.0	available
D3417-B2	R1.19.0	available	R1.19.0	available
D3433-S1	R1.23.0	available	R1.23.0	available
D3433-S2	R1.20.0	available	R1.20.0	available
D3434-S1	R1.23.0	available	R1.23.0	available
D3434-S2	R1.20.0	available	R1.20.0	available
D3441-S1	R1.23.0	available	R1.23.0	available
D3441-S2	R1.20.0	available	R1.20.0	available
D3445-S1	R1.23.0	available	R1.23.0	available
D3446-S1	R1.23.0	available	R1.23.0	available
D3446-S2	R1.20.0	available	R1.20.0	available
D3474-Bx	R1.9.0	available	R1.9.0	available
D3598-B1	R1.7.0	available	R1.7.0	available
D3633-S1	R1.2.0	available	R1.2.0	available
D3634-S1	R1.2.0	available	R1.2.0	available
D3641-S1	R1.1.0	available	R1.1.0	available
D3642-B1	R1.2.0	available	R1.2.0	available
D3643-H1	R1.2.0	available	R1.2.0	available
D3644-B1	R1.2.0	available	R1.2.0	available

D3646-S1	R1.1.0	available	R1.1.0	available
D3674-B1	R1.6.0	available	R1.6.0	available

Desktop PC (ESPRIMO)

	CVE-2018-3655,-3657, -3658,-3659		CVE-2018-3616	
System	New BIOS (with fix)	BIOS release date	New BIOS (with fix)	BIOS release date
ESPRIMO D556 (E94+ PPC)	R1.27.0	available	R1.27.0	available
ESPRIMO C720	---	---	R1.46.0	available
ESPRIMO D556 (E85+;E90+)	R1.27.0	available	R1.27.0	available
ESPRIMO D556/2 (E85+;E90+)	R1.19.0	available	R1.19.0	available
ESPRIMO D756 (E85+;E90+;E94+)	R1.27.0	available	R1.27.0	available
ESPRIMO D757 (E85+;E90+;E94+)	R1.19.0	available	R1.19.0	available
ESPRIMO D956 (E85+;E90+;E94+;LL)	R1.27.0	available	R1.27.0	available
ESPRIMO D957 (E85+;E90+;E94+)	R1.19.0	available	R1.19.0	available
ESPRIMO D958	R1.6.0	available	R1.6.0	available
ESPRIMO E420/P420/PH320	---	---	R1.46.0	available
ESPRIMO E520/P520	---	---	R1.46.0	available
ESPRIMO E720/P720	---	---	R1.46.0	available
ESPRIMO E920/P920/PH521	---	---	R1.46.0	available
ESPRIMO K557 (20", 24")	R1.9.0	available	R1.9.0	available
ESPRIMO K558	R1.6.0	available	R1.6.0	available
ESPRIMO P556/PH556	R1.27.0	available	R1.27.0	available
ESPRIMO P556/2	R1.19.0	available	R1.19.0	available
ESPRIMO P557	R1.19.0	available	R1.19.0	available
ESPRIMO P558/D558-8L	R1.6.0	available	R1.6.0	available
ESPRIMO P756 (E85+;E90+;E94+)	R1.27.0	available	R1.27.0	available
ESPRIMO P757 (E85+;E90+;E94+)	R1.19.0	available	R1.19.0	available
ESPRIMO P758/D758-8L	R1.6.0	available	R1.6.0	available
ESPRIMO P956 (E85+;E90+;E94+;LL)	R1.27.0	available	R1.27.0	available
ESPRIMO P957 (E85+;E90+;E94+;POWER)	R1.19.0	available	R1.19.0	available
ESPRIMO P958	R1.6.0	available	R1.6.0	available
ESPRIMO Q520	---	---	R1.46.0	available
ESPRIMO Q556	R1.27.0	available	R1.27.0	available
ESPRIMO Q556/2	R1.19.0	available	R1.19.0	available
ESPRIMO Q920, Q920/MRE	---	---	R1.46.0	available
ESPRIMO Q956	R1.27.0	available	R1.27.0	available
ESPRIMO Q956, Q956/MRE	R1.27.0	available	R1.27.0	available
ESPRIMO Q957, Q957/MRE	R1.19.0	available	R1.19.0	available
ESPRIMO X923 / X923T	---	---	R1.46.0	available
ESPRIMO X956	R1.27.0	available	R1.27.0	available
Team PoS 7000S	---	---	R1.46.0	available

Workstation (CELSIUS)

	CVE-2018-3655,-3657, -3658,-3659		CVE-2018-3616	
System	New BIOS (with fix)	BIOS release date	New BIOS (with fix)	BIOS release date
CELSIUS J550	R1.27.0	available	R1.27.0	available
CELSIUS J550/2	R1.19.0	available	R1.19.0	available
CELSIUS J580	R1.6.0	available	R1.6.0	available
Celsius M770	R1.7.0	available	R1.7.0	available
Celsius R970	R1.8.0	available	R1.8.0	available
CELSIUS W530	---	---	R1.46.0	available
CELSIUS W550, W550power	R 1.27.0	available	R 1.27.0	available
CELSIUS W570, POWER, POWER+	R1.19.0	available	R1.19.0	available
CELSIUS W580	R1.6.0	available	R1.6.0	available

Mobile (LIFEBOOK/STYLISTIC/CELSIUS)

	CVE-2018-3655,-3657, -3658,-3659		CVE-2018-3616	
System	New BIOS (with fix)	BIOS release date	New BIOS (with fix)	BIOS release date
LIFEBOOK A357	2.04	available	2.04	available
LIFEBOOK A357-SKL	3.03	available	3.03	available
LIFEBOOK A556 / A556G	V1.27	available	V1.27	available
LIFEBOOK A557	1.12	available	1.12	available
LIFEBOOK E448	1.13	available	1.13	available
LIFEBOOK E458	1.13	available	1.13	available
LIFEBOOK E546 non vPro	1.31	available	1.31	available
LIFEBOOK E546 vPro	1.22	available	1.22	available
LIFEBOOK E556 non vPro	1.31	available	1.31	available
LIFEBOOK E556 vPro	1.22	available	1.22	available
LIFEBOOK E547 non vPro	1.12	available	1.12	available
LIFEBOOK E547 vPro	1.16	available	1.16	available
LIFEBOOK E557 non vPro	1.12	available	1.12	available
LIFEBOOK E557 vPro	1.16	available	1.16	available
LIFEBOOK E548	1.16	available	1.16	available
LIFEBOOK E558	1.13	available	1.13	available
LIFEBOOK E734 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK E734 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK E736 non vPro	1.33	available	1.33	available

LIFEBOOK E736 vPro	1.25	available	1.25	available
LIFEBOOK E744 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK E744 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK E746 non vPro	1.33	available	1.33	available
LIFEBOOK E746 vPro	1.25	available	1.25	available
LIFEBOOK E744 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK E744 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK E756 non vPro	1.33	available	1.33	available
LIFEBOOK E756 vPro	1.25	available	1.25	available
LIFEBOOK P727	1.15	available	1.15	available
LIFEBOOK P728	1.10	available	1.10	available
LIFEBOOK S904 vPro	1.27	available	1.27	available
LIFEBOOK S935	1.19	available	1.19	available
LIFEBOOK S936	1.21	available	1.21	available
LIFEBOOK S937	1.10	available	1.10	available
LIFEBOOK S938	1.11	available	1.11	available
LIFEBOOK T725	1.21	available	1.21	available
LIFEBOOK T726	1.18	available	1.18	available
LIFEBOOK T734 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK T734 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK T904	t.b.d.	t.b.d.	t.b.d.	t.b.d.
LIFEBOOK T935	1.21	available	1.21	available
LIFEBOOK T936	1.21	available	1.21	available
LIFEBOOK T937	1.16	available	1.16	available
LIFEBOOK T938	1.09	available	1.09	available
LIFEBOOK U727	1.22	available	1.22	available
LIFEBOOK U727 (6th Gen.)	1.09	available	1.09	available
LIFEBOOK U728	1.13	available	1.13	available
LIFEBOOK U745	1.23	available	1.23	available
LIFEBOOK U747	1.22	available	1.22	available
LIFEBOOK U747 (6th Gen.)	1.09	available	1.09	available
LIFEBOOK U748	1.13	available	1.13	available
LIFEBOOK U757	1.22	available	1.22	available
LIFEBOOK U757 (6th Gen.)	1.09	available	1.09	available
LIFEBOOK U758	1.13	available	1.13	available
LIFEBOOK U904	1.18	available	1.18	available
LIFEBOOK U937	1.13	available	1.13	available
LIFEBOOK U938	1.14	available	1.14	available
STYLISTIC Q616	1.15	available	1.15	available
STYLISTIC Q665	1.17	available	1.17	available
STYLISTIC Q704 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
STYLISTIC Q704 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
STYLISTIC Q736	1.18	available	1.18	available
STYLISTIC Q737	1.14	available	1.14	available

STYLISTIC Q738	1.07	available	1.07	available
STYLISTIC Q775	1.22	available	1.22	available
STYLISTIC R726 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
STYLISTIC R726 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
STYLISTIC R727 non vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
STYLISTIC R727 vPro	t.b.d.	t.b.d.	t.b.d.	t.b.d.
STYLISTIC V727	1.15	available	1.15	available
CELSIUS H730	t.b.d.	t.b.d.	t.b.d.	t.b.d.
CELSIUS H760	1.27	available	1.27	available
CELSIUS H770	1.14	available	1.14	available
CELSIUS H780	1.04	available	1.04	available
CELSIUS H970	1.13	available	1.13	available
CELSIUS H980	1.08	available	1.08	available

PRIMERGY/PRIMEQUEST Server

	CVE-2018-3643,-3655,-3657, -3658		CVE-2018-3616, 3659
Affected Model	New BIOS (w/ fix)	BIOS release date	New BIOS (w/fix)
PRIMERGY BX920 S2	Not affected	Not relevant	Not affected
PRIMERGY BX922 S2	Not affected	Not relevant	Not affected
PRIMERGY BX924 S2	Not affected	Not relevant	Not affected
PRIMERGY BX920 S3	Not affected	Not relevant	Not affected
PRIMERGY BX924 S3	Not affected	Not relevant	Not affected
PRIMERGY BX920 S4	Not affected	Not relevant	Not affected
PRIMERGY BX924 S4	Not affected	Not relevant	Not affected
PRIMERGY BX2560 M1	Not affected	Not relevant	Not affected
PRIMERGY BX2580 M1	Not affected	Not relevant	Not affected
PRIMERGY BX2560 M2	Not affected	Not relevant	Not affected
PRIMERGY BX2580 M2	Not affected	Not relevant	Not affected
PRIMERGY CX250 S1	Not affected	Not relevant	Not affected
PRIMERGY CX270 S1	Not affected	Not relevant	Not affected
PRIMERGY CX272 S1	Not affected	Not relevant	Not affected
PRIMERGY CX250 S2	Not affected	Not relevant	Not affected
PRIMERGY CX270 S2	Not affected	Not relevant	Not affected
PRIMERGY CX2550 M1	Not affected	Not relevant	Not affected
PRIMERGY CX2570 M1	Not affected	Not relevant	Not affected
PRIMERGY CX2550 M2	Not affected	Not relevant	Not affected
PRIMERGY CX2570 M2	Not affected	Not relevant	Not affected
PRIMERGY CX2550 M4	R1.33.0	available	Not affected
PRIMERGY CX2560 M4	R1.33.0	available	Not affected
PRIMERGY CX2570 M4	R1.33.0	available	Not affected
PRIMERGY CX1640 M1	Not affected	Not relevant	Not affected
PRIMERGY MX130 S2	Not affected	Not relevant	Not affected

PRIMERGY RX100 S7	Not affected	Not relevant	Not affected
PRIMERGY RX100 S7p	Not affected	Not relevant	Not affected
PRIMERGY RX100 S8	Not affected	Not relevant	Not affected
PRIMERGY RX1330 M1	Not affected	Not relevant	Not affected
PRIMERGY RX1330 M2	Not affected	Not relevant	Not affected
PRIMERGY RX1330 M3	Not affected	Not relevant	Not affected
PRIMERGY RX200 S6	-	No update – End of Service	-
PRIMERGY RX200 S7	Not affected	Not relevant	Not affected
PRIMERGY RX200 S8	Not affected	Not relevant	Not affected
PRIMERGY RX2510 M2	Not affected	Not relevant	Not affected
PRIMERGY RX2520 M1	Not affected	Not relevant	Not affected
PRIMERGY RX2520 M4	R.1.28.0	available	Not affected
PRIMERGY RX2530 M1	Not affected	Not relevant	Not affected
PRIMERGY RX2530 M2	Not affected	Not relevant	Not affected
PRIMERGY RX2530 M4	R.1.28.0	available	Not affected
PRIMERGY RX300 S6	Not affected	Not relevant	Not affected
PRIMERGY RX300 S7	Not affected	Not relevant	Not affected
PRIMERGY RX300 S8	Not affected	Not relevant	Not affected
PRIMERGY RX2540 M1	Not affected	Not relevant	Not affected
PRIMERGY RX2540 M2	Not affected	Not relevant	Not affected
PRIMERGY RX2540 M4	R.1.28.0	available	Not affected
PRIMERGY RX350 S7	Not affected	Not relevant	Not affected
PRIMERGY RX350 S8	Not affected	Not relevant	Not affected
PRIMERGY RX2560 M1	Not affected	Not relevant	Not affected
PRIMERGY RX2560 M2	Not affected	Not relevant	Not affected
PRIMERGY RX4770 M1	Not affected	Not relevant	Not affected
PRIMERGY RX4770 M2	Not affected	Not relevant	Not affected
PRIMERGY RX4770 M3	Not affected	Not relevant	Not affected
PRIMERGY RX4770 M4	R.1.18.0	available	Not affected
PRIMERGY RX500 S7	Not affected	Not relevant	Not affected
PRIMERGY RX600 S6	Not affected	Not relevant	Not affected
PRIMERGY RX900 S1	Not affected	Not relevant	Not affected
PRIMERGY RX900 S2	Not affected	Not relevant	Not affected
PRIMERGY TX100 S3p	Not affected	Not relevant	Not affected
PRIMERGY TX1310 M1	Not affected	Not relevant	Not affected
PRIMERGY TX1310 M3	Not affected	Not relevant	Not affected
PRIMERGY TX140 S1p	Not affected	Not relevant	Not affected
PRIMERGY TX140 S2	Not affected	Not relevant	Not affected
PRIMERGY TX150 S7	Not affected	Not relevant	Not affected
PRIMERGY TX150 S8	Not affected	Not relevant	Not affected
PRIMERGY TX1320 M1	Not affected	Not relevant	Not affected
PRIMERGY TX1320 M2	Not affected	Not relevant	Not affected
PRIMERGY TX1320 M3	Not affected	Not relevant	Not affected

PRIMERGY TX120 S3p	Not affected	Not relevant	Not affected
PRIMERGY TX200 S6	Not affected	Not relevant	Not affected
PRIMERGY TX200 S7	Not affected	Not relevant	Not affected
PRIMERGY TX1330 M1	Not affected	Not relevant	Not affected
PRIMERGY TX1330 M2	Not affected	Not relevant	Not affected
PRIMERGY TX1330 M3	Not affected	Not relevant	Not affected
PRIMERGY TX300 S6	Not affected	Not relevant	Not affected
PRIMERGY TX300 S7	Not affected	Not relevant	Not affected
PRIMERGY TX300 S8	Not affected	Not relevant	Not affected
PRIMERGY SX150 S8	Not affected	Not relevant	Not affected
PRIMERGY SX350 S8	Not affected	Not relevant	Not affected
PRIMERGY TX2540 M1	Not affected	Not relevant	Not affected
PRIMERGY TX2550 M4	R.1.28.0	available	Not affected
PRIMERGY TX2560 M1	Not affected	Not relevant	Not affected
PRIMERGY TX2560 M2	Not affected	Not relevant	Not affected
PRIMEQUEST 2400E	Not affected	Not relevant	Not affected
PRIMEQUEST 2800B	Not affected	Not relevant	Not affected
PRIMEQUEST 2800E	Not affected	Not relevant	Not affected
PRIMEQUEST 2400E2	Not affected	Not relevant	Not affected
PRIMEQUEST 2800B2	Not affected	Not relevant	Not affected
PRIMEQUEST 2800E2	Not affected	Not relevant	Not affected
PRIMEQUEST 2400E3	Not affected	Not relevant	Not affected
PRIMEQUEST 2800B3	Not affected	Not relevant	Not affected
PRIMEQUEST 2800E3	Not affected	Not relevant	Not affected
PRIMEQUEST 3400E	Not affected	Not relevant	Not affected
PRIMEQUEST 3800B	R1.69.0	available	Not affected
PRIMEQUEST 3800E	Not affected	Not relevant	Not affected

* cw: calendar week

All rights reserved, including intellectual property rights.
Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.
For further information see ts.fujitsu.com/terms_of_use.html
© 2018 Fujitsu Technology Solutions GmbH