av1_data_trans

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2
av1_inject	vulnerable: 1 / not vulnerable: 0	inject new data to the stream	1	1	1	1	1	1
av1_replay	vulnerable: 1 / not vulnerable: 0	finding some way to replay information to the server	1	1	0	0	1	1
av1_ssl	not using SSL: 1 / using SSL: 0	is using SSL	0	0	1	0	1	0
av1_ssl_forg	vulnerable: 1 / not vulnerable: 0	secure and correct implementation of communication encryption	1	0	1	0	1	0
av1_ssl_forg_ca	vulnerable: 1 / not vulnerable: 0	in addition to data_com_ssl_forg the trusted CA certificate is installed	1	1	1	0	1	1
av1_tamper	not vulnerable: 0 / upper limit e.g. weight: 1 / no limit or validation: 2	tampering the data before it can reach the server defeating input validation	2	1 no limit	2	1	2	2
			6.0	4.0	6.0	2.0	7.0	5.0

av2_mobile_device

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2
av2_export_backup	data not encrypted: 2 / data in backup encrypted: 1 / no data stored: 0	data is being backed up using the android backup command	0	2	2	1	2	2
av2_export_logging	information available: 1 / no information: 0	investigate the Android log for unencrypted information	0	0	1	0	1	0
			0.0	2.0	3.0	1.0	3.0	2.0

av3_mobile_app

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2
av3_code_comment	informational	any comment on the code		tbd				
av3_data_coll	informational	data collected and send by the mobile app						
av3_data_leakage	no data leaked: 0 / complies with privacy policy: 1 / data leaked beyond privacy policy: 2	identifiable for the user or the phone that is being collected	2	0	2	1	2	1
av3_data_wipe	unsecure feature: 1 / secure feature: 0	can data be wiped from the mobile application	1	1	1	1	1	1

av3_export_cloud	unsecure feature: 1 / secure feature: 0	data being exported somewhere into the cloud (dropbox et al)	n/a	n/a	n/a	n/a	n/a	n/a
av3_export_sdcard	unsecure feature: 1 / secure feature: 0	can data be exported to SD card or other locations on device and is that data encrypted	n/a	n/a	n/a	n/a	n/a	n/a
av3_export_social	unsecure feature: 1 / secure feature: 0	export variants to social media and data encryption while exporting	n/a	0	0	n/a	0	n/a
av3_pwd_change_freq	no period or frequency: 2 / either one: 1 / both: 0	password change period (must) and frequency (can)	n/a	n/a	2	n/a	2	2
av3_pwd_change_policy	no policy: 0 / min characters: 1 / mixed charsets: 2	password policy enforced on password change	n/a	n/a	1	n/a	1	n/a
av3_pwd_change_reuse	yes, unlimited: 0 / no, but history can be bypassed (see change freq): 1 / no without limitation: 2	can a password be reused and how much difference is required	n/a	n/a	1	n/a	2	n/a
av3_reg_acc_verif	none: 2 / email account verification: 1 / two factor authentication 0	email account verification or two factor authentication	2	n/a	2	2	2	2
av3_reg_data_input	informational	Specifies the data fields and types which are required as inputs		n/a				
av3_reg_data_validation	data not validated: 1 / data is validated: 0	Comments on data validation during user registration: weight, heitght, email...	0	n/a	0	0	0	0
av3_reg_pripol_link	no link or information: 1 / link available: 0	link to privacy policy or any kind of information on such topic	0	n/a	1	1	1	0
av3_reg_pwd_policy	no policy: 2 / min characters: 1 / mixed charsets: 0	is a password policy enforced	2	n/a	1	1	1	2
			7.0	1.0	11.0	6.0	12.0	8.0

av4_third_party

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2
av4_data_leakage	no data leaked: 0 / complies with privacy policy: 1 / data leaked beyond privacy policy: 2	data leakage to third party services	1	0	1	0	1	0
			1.0	0.0	1.0	0.0	1.0	0.0

av5_sensor_device

test step	rating	desc	Activ8rLives Body Analyser com.activ8rlives.mobile	FitBit aria com.fitbit.FitbitMobile	HAPI Connected Scale com.hapiconnect	iChoice S1 com.medm.medmwt.diary	Thomson TBS705 com.stabxtom.thomson	Withings WS-30 com.withings.wiscale2
av5_data_coll	informational	characteristics of data collected by the sensor						
av5_pairing_process	informational	pairing process between sensor and phone						
av5_swfw_update	vulnerable: 1 / not vulnerable: 0	update cycle related issues	1	0	1	1	1	0
			1.0	0.0	1.0	1.0	1.0	0.0

av6_web_application

Body Analyser obile bile ted Scale wt.diary 705 mson 30 ale2

test step	rating	desc	Activ8rLives B com.activ8rlives.m	FitBit aria com.fitbit.FitbitMob	HAPI Connect com.hapiconnect	iChoice S1 com.medm.medmw	Thomson TBS com.stabxtom.tho	Withings WS- com.withings.wisc
av6_csrf	vulnerable: 1 / not vulnerable: 0	basic CSRF attack	1	0	0	0	n/a	0
av6_data_input	data not validated: 1 / data is validated: 0	data input via web UI and validation	0	0	1	1	n/a	0
av6_data_wipe	insecure feature: 1 / secure feature: 0	wipe and delete data from the web account	1	0	0	0	n/a	0
av6_export_cloud	insecure feature: 1 / secure feature: 0	data being exported somewhere into the cloud (dropbox et al)	n/a	n/a	n/a	n/a	n/a	n/a
av6_export_disk	insecure feature: 1 / secure feature: 0	can data be exported to SD card or other locations on device and is that data encrypted	0	0	n/a	0	n/a	0
av6_export_social	insecure feature: 1 / secure feature: 0	export variants to social media and data encryption while exporting	n/a	0	0	n/a	n/a	n/a
av6_pri_pol	no link or information: 1 / link available: 0	pirvacy poclicy linked and available	0	0	0	0	n/a	0
av6_pwd_change_freq	no period or frequency: 2 / either one: 1 / both: 0	password change period (must) and frequency (can)	2	2	2	2	n/a	2
av6_pwd_change_policy	no policy: 2 / min characters: 1 / mixed charsets: 0	password policy enforced on password change	2	1	1	1	n/a	1
av6_pwd_change_reuse	yes, unlimited: 0 / no, but history can be bypassed (see change freq): 1 / no without limitation: 2	can a password be reused and how much difference is required	2	2	2	2	n/a	2
av6_reg_acc_verif	none: 2 / email account verification: 1 / two factor	email account verification or two factor authentication	2	1	2	1	n/a	2

	authentication 0							
av6_reg_data_input	informational	Specifies the data fields and types which are required as inputs					n/a	
av6_reg_data_validation	data not validated: 1 / data is validated: 0	Comments on data validation during user registration: weight, heitght, email...	0	0	1	0	n/a	0
av6_reg_pripol_link	no link or information: 1 / link available: 0	link to privacy policy or any kind of information on such topic	1	0	1	0	n/a	0
av6_reg_pwd_policy	no policy: 2 / min characters: 1 / mixed charsets: 0	is a password policy enforced	2	1	1	1	n/a	1
av6_sql_injection	vulnerable: 1 / not vulnerable: 0	inject sql queries to learn information from the server	0	0	0	0	n/a	0
av6_xss	vulnerable: 1 / not vulnerable: 0	basic xss attacks on the web page with a select statement	0	0	0	0	n/a	0
			13.0	7.0	11.0	8.0	0.0	8.0

sol_arch

device package	comment
com.fitbit.FitbitMobile FitBit aria	pairing works as described via wifi and connecting to the scale directly; scale communicates via unencrypted wifi connection with the fitbit server and sends information to them; scale and protocol have been researched by others and fitbit has already improved on their weaknesses a lot
com.stabxtom.thomson Thomson TBS705	measurements from the scale are first inserted into the database and then synchronized to a server (data center); however once the data has been synchronized to that server it is not any longer accessible for the user; the app after reset does not load the already collected data initially
com.withings.wiscale2 Withings WS-30	scale can connect via wifi and bluetooth wifi option enables scale to communicate with withings immediately wifi option is using http only phone is loading data from webservice scale is set up via bluetooth, this way it is provided with parameter