

av1_data_trans

test step	rating	desc					
			com.activ8rives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabtom.thomson	com.withings.wiscale2
av1_inject	vulnerable: 0 / not vulnerable: 1	inject new data to the stream	0	0	0	0	0
av1_replay	vulnerable: 0 / not vulnerable: 1	finding some way to replay information to the server	0	1	1	0	0
av1_ssl_forg	vulnerable: 0 / not vulnerable: 1	secure and correct implementation of communication encryption	0	0	1	0	1
av1_ssl_forg_ca	vulnerable: 0 / not vulnerable: 1	in addition to data_com_ssl_forg the trusted CA certificate is installed	0	0	1	0	0
av1_tamper	not vulnerable: 2 / upper limit e.g. weight: 1 / no limit or validation: 0	tampering the data before it can reach the server defeating input validation	0	0	1	0	0
			0.0	1.0	4.0	0.0	1.0

av2_mobile_device

test step	rating	desc					
			com.activ8rives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabtom.thomson	com.withings.wiscale2
av2_export_backup	data not encrypted: 0 / data in backup encrypted: 1 / no data stored: 2	data is being backed up using the android backup command	2	0	1	0	0
av2_export_logging	information in log available or not	investigate the Android log for unencrypted information	1	0	1	0	1
			3.0	0.0	2.0	0.0	1.0

av3_mobile_app

test step	rating	desc					
			com.activ8lives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabxtom.thomson	com.withings.wiscale
av3_code_comment	general comment on coding	any comment on the code					
av3_data_coll	informational	data collected and send by the mobile app					
av3_data_leakage	no data leaked: 2 / complies with privacy policy: 1 / data leaked beyond privacy policy: 0	identifiable for the user or the phone that is being collected	0	0	1	0	1
av3_data_wipe	unsecure feature: 0 / secure feature: 1	can data be wiped from the mobile application	0	0	0	0	0
av3_export_cloud	unsecure feature: 0 / secure feature: 1	data being exported somewhere into the cloud (dropbox et al)	n/a	n/a	n/a	n/a	n/a
av3_export_sdcard	unsecure feature: 0 / secure feature: 1	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
av3_export_social	unsecure feature: 0 / secure feature: 1	export variants to social media and data encryption while exporting	n/a	1	n/a	1	n/a
av3_pwd_change_freq	0 no rule 1 rule but not reasonable (> 90 days) 2 rule and reasonable (< 90 days)	password change period (must) and frequency (can)	n/a	0	n/a	0	0
av3_pwd_change_policy	0 - no policy 1 - min characters 2 - mixed charsets	password policy enforced on password change	n/a	1	n/a	1	n/a
av3_pwd_change_reuse	0 - yes, unlimited 1 - no, but history can be bypassed (see change freq) 2 - no without limitation	can a password be reused and how much difference is required	n/a	1	n/a	0	n/a
av3_reg_acc_verif	0 / none 1 / email account verification 2 / two factor authentication	email account verification or two factor authentication	0	0	0	0	0
av3_reg_data_input	informational	Specifies the data fields and types which are required as inputs					
av3_reg_data_validation	0 - data not validated; 1 - data is validated	Comments on data validation during user registration: weight, height, email...	1	1	1	1	1
av3_reg_pripol_link	0 - no link or information; 1 - link available	link to privacy policy or any kind of information on such topic	1	0	0	0	1
av3_reg_pwd_policy	0 - no policy 1 - min characters 2 - mixed charsets	is a password policy enforced	0	1	1	1	0
			2.0	5.0	3.0	4.0	3.0

av4_third_party

test step	rating	desc	com.activ8lives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabxtom.thomson	com.withings.wiscale2
av4_data_leakage	1 - no data leaked/complies privacy policy; 0 - data leaked beyond privacy policy	data leakage to third party services	0	0	1	0	1
			0.0	0.0	1.0	0.0	1.0

av5_sensor_device

test step	rating	desc	com.activ8lives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabxtom.thomson	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	0 - vulnerable 1 - not vulnerable	update cycle related issues	0	0	0	0	1
			0.0	0.0	0.0	0.0	1.0

av6_web_application

test step	rating	desc					
			com.activ8lives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabxtom.thomson	com.withings.wiscalec
av6_csrf	0 - vulnerable 1 - not vulnerable	basic CSRF attack	0	1	1	n/a	1
av6_data_input	0 - data not validated; 1 - data is validated	data input via web UI and validation	1	0	0	n/a	1
av6_data_wipe	unsecure feature: 0 / secure feature: 1	wipe and delete data from the web account	0	1	1	n/a	1
av6_export_cloud	unsecure feature: 0 / secure feature: 1	data being exported somewhere into the cloud (dropbox et al)	n/a	n/a	n/a	n/a	n/a
av6_export_disk	unsecure feature: 0 / secure feature: 1	can data be exported to SD card or other locations on device and is that data encrypted	1	n/a	1	n/a	1
av6_export_social	unsecure feature: 0 / secure feature: 1	export variants to social media and data encryption while exporting	n/a	1	n/a	n/a	n/a
av6_pri_pol	0 not available; link available 1	privacy poclcy linked and available	1	1	1	n/a	1
av6_pwd_change_freq	0 no rule 1 rule but not reasonable (> 90 days) 2 rule and reasonable (< 90 days)	password change period (must) and frequency (can)	0	0	0	n/a	0
av6_pwd_change_policy	0 - no policy 1 - min characters 2 - mixed charsets	password policy enforced on password change	0	1	1	n/a	1
av6_pwd_change_reuse	0 - yes, unlimited 1 - no, but history can be bypassed (see change freq) 2 - no without limitation	can a password be reused and how much difference is required	0	0	0	n/a	0
av6_reg_acc_verif	0 / none 1 / email account verification 2 / two factor authentication	email account verification or two factor authentication	0	0	0	n/a	0
av6_reg_data_input	informational	Specifies the data fields and types which are required as inputs				n/a	
av6_reg_data_validation	0 - data not validated; 1 - data validated	Comments on data validation during user registration: weight, height, email...	1	0	1	n/a	1
av6_reg_pripol_link	0 - no link or information; 1 - link available	link to privacy policy or any kind of information on such topic	0	0	0	n/a	1
av6_reg_pwd_policy	0 - no policy 1 - min characters 2 - mixed charsets	is a password policy enforced	0	1	1	n/a	1
av6_sql_injection	vulnerable: 0 / 1	inject sql queries to learn information from the server	1	0	0	n/a	1
av6_xss	vulnerable: 0 / 1	basic xss attacks on the web page with a select statement	0	0			