

av1_data_trans

test step	rating	desc	com.activ8rives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabtom.thomson	com.withings.w
av1_inject	vulnerable: 0 / not vulnerable: 1	inject new data to the stream	0 requests with new measurements are not authenticated and measurements are mapped by userid; so as soon as one finds out a user ID measurements can be happily inserted	0 injection is possible with reconstructing the signature value.. all required values can be read from the communication stream	0 injection is only possible as long as the user provides an authenticated session	0 injection is possible	0 possible as long as scale has session and this can be used
av1_replay	vulnerable: 0 / not vulnerable: 1	finding some way to replay information to the server	0 replaying of messages is easliy possible but will replace the existing record for a day as only one record per day can exist	1 simple replay is not possible due to client side generated signatures	1 replay is not possible as every record comes with a separate uuid	0 replay attacks are perfectly possible even with stolen session ID.. however the generated data seems to be unaccessible to the user	0 replay attacks are possible within the same session session is requested based on a once which is used to generate a hash the server is able to use that hash to identify the user and sends user information including a valid session key
av1_ssl_forg	vulnerable: 0 / not vulnerable: 1	secure and correct implementation of communication encryption	0 working - username and password in message body clear text	0 no SSL usage	1 not working	0 working - username in clear text, mobile id and password somehow encrypted or obfuscated	1 not working
av1_ssl_forg_ca	vulnerable: 0 / not vulnerable: 1	in addition to data_com_ssl_forg the trusted CA certificate is installed	0 working as without CA certificate	0 NO SSL - username in cleartext and password	1 not working	0 NO SSL	0 working

				somehow encrypted or obfuscated			
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 tampering with the weight data is possible a weight up to 99999999 kg can be entered; beyond that the server will respond with an error	0 possible at any point in time	1 records can be changed but still the max weight is validated and limited to 300kg	0 data can be easily changed and is happily accepted by the server	0 data can be changed and apparently the server is not validating the data so that unplausible data can be entered tried to change the user ID so that the data would be inserted into a different account -> that however was not successful
			0.0	1.0	4.0	0.0	1.0

av2_mobile_device

test step	rating	desc	com.activ8lives.mobile	com.hapiconnect	com.medm.medmwt.diary	com.stabxtom.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 no data in backup found	0 database unencrypted, password in clear text in shared prefs,	1 sqlite databases not encrypted; shared preferences are obscured and encrypted	0 backup contains unencrypted database which includes all information from measurements to device information / information on session and any credentials can be picked up from the shared prefs folder	0 database is available and data can be read in clear text
av2_export_logging	information in log available or not	investigate the Android log for unencrypted information	1 no suspicious data in logging information	0 logging contains detailed information on every single request send to the server	1 no information leaked in logcat	0 logcat shows detailed logs with even some information on the recorded data and partly http traces bluetooth connection management is shown in full including MAC addresses which are logged and saved	1 no information written to logcat
			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.wiscale2
		app crashing with Android 6.0.1 so reverting back to Android 6 also App is Xamarin based and running in Monodroid VM on Android which is some C style based	passwords are just hased with MD5 no salt; after re login signature looks suspicious as no password is transmitted - seems to be	code is somewhat supprinsingly just a few lines and decompiled code doesn't show all the information hence something must have	code shows many different frameworks and addons integrated with the solution (also see addons table) the app itself shows less possibilities to make actually	tbd	

av3_code_comment	general comment on coding	any comment on the code	implementation	generated based on current time, previous access token and some generat random number; but all this information is available to an attacker	been applied to the code also certificate pinning is implemented and had to be removed in order to run further tests	use of these frameworks and addons the password seems to be MD5 hashed but since the communication is not encrypted and the hash is not randomiyed that is pointless, simply use the hash value to execute anything	
av3_data_coll	informational	data collected and send by the mobile app	normal data collection of pictures and other details on the phone	not possible to enter data manually	manual input only and photo capture to set profile picture	as mentioned app collecteds weight data but also sends phone identifier to china	added entry manually to be uploaded to server API with server seems to be different from the scales API query parameters instead of body but everything is SSL encrypted some input validation inside the mobile application is done; manual entries are possible; no othe seems to be transmitted
av3_data_leakage	no data leaked: 2 / complies with privacy policy: 1 / data leaked beyond privacy policy: 0	identifiabale for the user or the phone that is being collected	0 xamarin framework is sending the android device id home and is tracking different events such as network change from wifi to lte, application startup and a full device fingerprint including attributes such as screen size, resolution, network, model, memory, cpu count, android version, client version, app installed	0 no SSL implemented so data can easily be read; in addition passwords are just MD5 hashed without salts what makes them vulnerable to rainbow table lookups; full personal information including email address, password, date of birth, weight and height can be read	1 as far as captured no data was being leaked	0 !! advertising library Umeng detected.. library is sending a full device fingerprint including IMEI and MAC (where it cant retrieve the MAC because of Android 6 changes) /n password (encrypted) and email send over unencrypted network; password seems to be some kind of 16byte hash.. tried a few tools to get the pattern and reproduce it but so far without success reveals full details during pairing as serial numbers, device hardware version, software version and some specific password are sent unencrypted	1 none

av3_data_wipe	unsecure feature: 0 / secure feature: 1	can data be wiped from the mobile application	0 no possibility to wipe data from inside the app	0 not possible from within the app	0 no data wipe option	0 no data wipe from within the app only be using the system settings; also no possibility to delete data from the server and hard to contact them as there is no email received or any information inside the app leading to a contact address	0 no possibility to wipe data from app or from device, no way to delete account
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 screenshots can be exported which show some graph with weight overview	n/a n/a	n/a no possibility	n/a no export option in app
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 n/a	n/a no option	n/a no export option
av3_export_social	unsecure feature: 0 / secure feature: 1	export variants to social media and data encryption while exporting	n/a n/a	1 screenshot of the graph can be shared with any 3rd party app	n/a n/a	1 twitter, facebook and email but none of them worked	n/a sharing is just inviting and as such possible to gmail, drive, bluetooth and android beam
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 can't change password from within the app	0 nothing enforced	n/a n/a	0 no password change policy or frequency enforced	0 n/a
av3_pwd_change_policy	0 - no policy 1 - min characters 2 - mixed charsets	password policy enforced on password change	n/a n/a	1 min 6 characters	n/a n/a	1 password policy is just 6 characters only and nothing else	n/a 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 n/a	1 last password can't be reused	n/a n/a	0 passwords can be reused at any point in time how often ever the user wants to	n/a n/a

av3_reg_acc_verif	0 / none 1 / email account verification 2 / two factor authentication	email account verification or two factor authentication	0 received no email on account verification / registration	0 not at all	0 no - but received email with pointers to privacy statements and similar stuff	0 no verification email received	0 there is no trace of account verification not even a single email was received assumption that this might be solution dependent as the withings watch caused a lot of spam in the inbox
av3_reg_data_input	informational	Specifies the data fields and types which are required as inputs	weight, height, waistline, birthdate and bio data, fitness goal and setps towards the goal basic validation on weight, height and waistline	username, email, weight and height, and password	only email address and password mandatory; name, birth date and height can be entered later from within the app	email, password, name, gender, name, birthday, height, weight, waistline, picture	select scale n email and password n firstname, lastname, birthdate, height, weight
av3_reg_data_validation	0 - data not validated; 1 - data is validated	Comments on data validation during user registration: weight, heitght, email...	1 basic validation on weight, height and waistline	1 weight and height only	1 height and weight are limited; no other validation	1 limited values for weight, height, waistline, age	1 email adress is validated n password provided A n very high weights are not allowed 600lb but weird error message n height is accepted at 3m
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 link to terms and conditions plus acceptance of terms and conditions is required to use the app	0 no explicit link visible	0 not visible during registration but linked from within the app	0 no link to privacy policy apparent	1 link to privacy policy is provided http://www.withings.com/uk/en/legal also terms and conditions but both links are pointing to the same webpage1
av3_reg_pwd_policy	0 - no policy 1 - min characters 2 - mixed charsets	is a password policy enforced	0 no password policy as registration with a simple A was possible	1 min 6 characters	1 min 6 character	1 6-16 characters	0 no hint to any kind of password policy could be found
			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 detailled data on the device is leaked to xamarin servers; this data can be used for fingerprinting and shouldn't be collected; there are other device identifiers that can be used /n pictures taken are uploaded to an image service and not to their own servers	0 no data leakage apparent	1 no data leakage to third party on recor d	0 data is being leaked to advertising companies; data includes phone identifier information	1 no data being leaked
			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.stabtom.thomson	com.withings
av5_data_coll	informational	characteristics of data collected by the sensor	collecting data from scale and transferring it immediately without any user interact the webservice	weight is collected and uploaded; as far as seen no other data is added	collects data from scale as expected and save's on device; after some time it will be synchronized to the server	collecting weight information just as expected	data is being transmitted via http only scale is able to display the weather of the day other then that it just collects a measurements with a UNIX timestamp and the weight in g this a JSON document being posted to the server also location information is send to the scale and used by it; this communication is encrypted
av5_pairing_process	informational	pairing process between sensor and phone	no pairing process as such as the scale doesn't authenticate itself with the app but communicates anonymously	pairing process is without real device pairing using a passcode or something	pairing comes again without real bluetooth pairing.. interestingly the device asks for location access rather than bluetooth access permission	no real pairing	pairing is possible via bluetooth to the phone; it requires an authentication and is persisted; thereafter the scale is able to communicate via wifi or bluetooth with the server
av5_swfw_update	0 - vulnerable 1 - not vulnerable	update cycle related issues	0 app to server communication doesn't show any hint regarding a firmware version for the scale	0 communication between app and server doesn't show any hint of information on possible firmware updates	0 no version information exchanged between app and server	0 scale sends its version on registration to the server but doesn't expect any updates	1 scale asks server if any firmware update is available and provides the currently installed version intercepting this request and changing the firmware yields a link to an update send by server
			0.0	0.0	0.0	0.0	1.0

av6_web_application

test step	rating	desc	com.activ8lives.mobi					com.hapiconnect					com.medn.medmnw					com.stabxtom.thon					com.withr				
av6_csrf	0 - vulnerable 1 - not vulnerable	basic CSRF attack	0 csrf token are not renewed after request so that if an attacker manages to steal one of them he is able to send requests for the duration of the session; csrf token is correctly bound to the session	1 tested on password change and found that websites protects against CSRF	1 not vulnerable.. is using authenticity tokens for requests	n/a n/a	1 protected																				
av6_data_input	0 - data not validated; 1 - data is validated	data input via web UI and validation	1 data is limited to max 300kg	0 data is not validated since unreasonably high measurements can be entered	0 data is not validated but sanitized	n/a n/a	1 limited																				
av6_data_wipe	unsecure feature: 0 / secure feature: 1	wipe and delete data from the web account	0 data wipe is not available from the web page; the policy mentions two mail addresses one for deactivation and one for deletion of which none worked; email send to again another mail address and waiting for response -> even worse managed to send an email from a different email account to delete another account	1 no option	1 account deletion possible	n/a n/a	1 account can be deleted but has 7 days period before they claim that data will actually be removed from their systems																				
av6_export_cloud	unsecure feature: 0 / secure feature: 1	data being exported somewhere into the cloud (dropbox et al)	n/a no export options	n/a n/a	n/a 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 excel document can be exported and data within that document is unencrypted	n/a n/a	1 download as csv or html page	n/a n/a	1 only after account deletion data can be downloaded
av6_export_social	unsecure feature: 0 / secure feature: 1	export variants to social media and data encryption while exporting	n/a no social sharing other than the web platforms own sharing is implemented; carer can be invited and also practitioners and clinics can get access; however that feature was not working	1 facebook, twitter	n/a only within the same platform	n/a n/a	n/a no hint that data can be shared online
av6_pri_pol	0 not available; link available 1	privacy policy linked and available	1 the privacy policy is linked from the web page	1 link in footer but not very visible	1 linked on web page	n/a n/a	1 visibly linked from web interface
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 not implemented	0 none	0 none	n/a n/a	0 no frequency enforced
av6_pwd_change_policy	0 - no policy 1 - min characters 2 - mixed charsets	password policy enforced on password change	0 none	1 6 characters	1 min 6 characters	n/a n/a	1 min 6 char; any char no type enforcement
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 none	0 unlimited	0 not limited	n/a n/a	0 unlimited reuse
av6_reg_acc_verif	0 / none 1 / email account verification 2 / two factor authentication	email account verification or two factor authentication	0 none	0 no	0 no.. just email with confirmation that account has been created	n/a n/a	0 no verification
av6_reg_data_input	informational	Specifies the data fields and types which are required as	same as app	name, email, date of birth,	same as app	n/a	same as mobile app

		inputs		goals		n/a	
av6_reg_data_validation	0 - data not validated; 1 - data validated	Comments on data validation during user registration: weight, height, email...	1 same as app: only medical data	0 no	1 same as app	n/a n/a	1 some data validation for height and weight
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 no explicit information	0 not visible but very hidden in footer	0 bottom of the page	n/a n/a	