Talos Vulnerability Report

TALOS-2020-1146

Dream Report platform privilege escalation vulnerability

APRIL 8, 2021

CVE NUMBER

CVE-2020-13532, CVE-2020-13533, CVE-2020-13534

Summary

Multiple privilege escalation vulnerabilities exist in Dream Report 5 R20-2. A specially crafted executable can cause elevated capabilities. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

Dream Report 5 R20-2

Product URLs

https://dreamreport.net/

CVSSv3 Score

9.3 - CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-276 - Incorrect Default Permissions

Details

Dream Report 5 R20-2 is a real-time reporting and charting solution. It collects and processes real-time information from variety of systems through a number of connectors which can be used for data import.

By default, Dream Report 5 R20-2 is installed in the `C:\ODS` directory with permissions that allows anyone on the system to have “full control” over certain files in the directory. This can lead to exploitable privilege escalations which can be triggered directly or indirectly by an attacker.

CVE-2020-13532 - Syncfusion Dashboard Service Privilege Escalation

In the default configuration, the `Syncfusion Dashboard Service` service binary can be replaced by attackers to escalate privileges to `NT SYSTEM`:

```
cacls "C:\ODS\Dream Report\Dashboard\Dashboard Platform SDK\Utilities\Windows Service\Syncfusion Dashboard Windows Service.exe"
C:\ODS\Dream Report\Dashboard\Dashboard Platform SDK\Utilities\Windows Service\Syncfusion Dashboard Windows Service.exe
BUILTIN\Administrators:(ID)F

Everyone:(ID)F
```

CVE-2020-13533 - ods_rtm_launch and ods_usc Run Key Privilege Escalation

In the default configuration, the following registry keys, which reference binaries with weak permissions, can be abused by attackers to effectively ‘backdoor’ the installation files and escalate privileges when a new user logs in and uses the application:

```
Registry Key (x86): HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ods_rtm_launch
Registry Key (x64): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ods_rtm_launch
Binary: C:\ODS\Dream Report\System\RTM.exe
Permission: cacls "C:\ODS\Dream Report\System\RTM.exe"
C:\ODS\Dream Report\System\Rtm.exe BUILTIN\Administrators:(ID)F
                                                        Everyone:(ID)F


Registry Key (x86): HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ods_usc
Registry Key (x64): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ods_usc
Binary: C:\ODS\Dream Report\System\usc.exe
Permission: cacls "C:\ODS\Dream Report\System\usc.exe"
C:\ODS\Dream Report\System\USC.exe BUILTIN\Administrators:(ID)F
                                                        Everyone:(ID)F
```

CVE-2020-13534 - DCOM Server Application Privilege Escalation

The following COM Class Identifiers (CLSID), installed by Dream Report 5 20-2, reference LocalServer32 and InprocServer32 with weak privileges which can lead to privilege escalation when used:

```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{CAB0B109-A3F4-44B8-AE0B-47C45DF8BCBC}\LocalServer32\LocalServer32
Binary:  C:\ODS\Dream Report\System\IDSEng.exe
Permission: cacls "C:\ODS\Dream Report\System\IDSEng.exe"
C:\ODS\Dream Report\System\IDSEng.exe BUILTIN\Administrators:(ID)F
                                                                Everyone:(ID)F


Key: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E3D65B93-2D26-41F1-B655-F14144C879B6}\InprocServer32\InprocServer32
Binary: C:\ODS\Dream Report\System\IISToolbox.dll
Permission: cacls "C:\ODS\Dream Report\System\IISToolbox.dll"
C:\ODS\Dream Report\System\IISToolbox.dll BUILTIN\Administrators:(ID)F
                                    Everyone:(ID)F
```

Timeline

2020-09-08 - Initial contact

2020-09-08 - Vendor acknowledged and provided PGP for communication

2020-09-09 - Vendor advised release planned for December 2020

2020-11-10 - Talos follow up with vendor to confirm Dec release

2020-11-18 - 2nd follow up

2020-11-30 - 3rd follow up

2021-01-04 - Final follow up

2021-01-15 - Vendor advised release pushed to “Q2 or early Q3”

2021-04-08 - Public disclosure

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1008

NEXT REPORT TALOS-2020-1201