Talos Vulnerability Report

TALOS-2021-1384

Dream Report ODS Remote Connector privilege escalation vulnerability

DECEMBER 6, 2021

CVE NUMBER

CVE-2021-21957

Summary

A privilege escalation vulnerability exists in the Remote Server functionality of Dream Report ODS Remote Connector 20.2.16900.0. A specially-crafted command injection can lead to elevated capabilities. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

Dream Report ODS Remote Connector 20.2.16900.0

Product URLs

https://dreamreport.net/

CVSSv3 Score

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

CWE

CWE-276 - Incorrect Default Permissions

Details

Dream Report is an automation platform designed to facilitate collection and parsing of real-time information between various devices in industrial environments.

The service ‘RTM Reporting System Runtime Manager’ is installed during stand-alone installation of ODS Remote Connector and starts with the following command (with high integrity):

```
 c:\program files (x86)\ods\remote connector\system\rtm.exe" -control -runMode svc
```

After above command line is executed, another binary is also started and runs throughout lifecycle of the main service process:

```
"C:\Program Files (x86)\ODS\Remote Connector\System\Rdxa.exe"
```

RTM Reporting System Runtime Manager allows any user on the system to replace a binary located in the default installation folder, as seen below, to execute code with privilege of NT SYSTEM with high integrity:

```
c:\program files (x86)\ods\remote connector\system\Rtm.exe:
BUILTIN\Administrators:(ID)F
Everyone:(ID)F

C:\Program Files (x86)\ODS\Remote Connector\System\Rdxa.exe:
BUILTIN\Administrators:(ID)F
Everyone:(ID)F
```

In addition, due to permission weaknesses, other components such as DLL libraries, used by any of the applications above, can be used to sideload code from the following folder:

```
C:\Program Files (x86)\ODS\Remote Connector\System
```

These can be, for example:

```
BatchManager.dll
ChangeManager.dll
FontManagerDll.dll
```

Note that initial exploitation would result in access to the same privilege as a default virtual service user `nt service\rtm reporting system runtime manager`. A full exploitation chain would need to take advantage of the `SeImpersonatePrivilege` privilege assigned to the RTM Reporting System Runtime Manager service to achieve reliable execution with NT SYSTEM privilage.

Vendor Response

Fixed in Dream Report Remote Connector 20.2.16900.1011

Timeline

2021-10-05 - Vendor Disclosure
2021-12-02 - Vendor patched
2021-12-06 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2021-1352

NEXT REPORT

TALOS-2021-1404