Talos Vulnerability Report

TALOS-2022-1490

Open Automation Software Platform Engine cleartext transmission of sensitive information vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26077

Summary

A cleartext transmission of sensitive information vulnerability exists in the OAS Engine configuration communications functionality of Open Automation Software OAS Platform V16.00.0112. A targeted network sniffing attack can lead to a disclosure of sensitive information. An attacker can sniff network traffic 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:H/I:N/A:N

CWE

CWE-319 - Cleartext Transmission of Sensitive Information

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 default all configuration communication with the OAS Platform is sent in cleartext over TCP/58727. Some configuration commands such as `SecureTransferFiles` require an OAS User account in an authorized OAS Security Group. When a command with this requirement, or any request from a logged-in OAS Configuration Utility, is sent, the username and base64 password hash is included in the message. If an attacker is sniffing the network during this time it would be possible to extract this information and subsequently use it to successfully send additional configuration commands that require credentials.

A `SecureTransferFiles` message showing these credentials 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 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/.....
```

Mitigation

The easiest way to mitigate attempts to exploit this vulnerability is to ensure that proper network segmentation is in place such that an attacker has the smallest possible access to the network on which the OAS Platform communicates. 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

NEXT REPORT

TALOS-2022-1491

TALOS-2022-1489