Talos Vulnerability Report

TALOS-2022-1494

Open Automation Software Platform Engine SecureBrowseFile information disclosure vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-27169

Summary

An information disclosure vulnerability exists in the OAS Engine SecureBrowseFile functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted network request can lead to a disclosure of sensitive information. An attacker can send a network request 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-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 properly-formatted unauthenticated configuration message to the OAS Platform, it is possible to get a directory listing at any location permissible by the underlying user. By default this message can be sent to TCP/58727 and, if successful, will be processed by the user `oasuser` with normal user permissions. When a `SecureBrowseFile` command is successfully processed, the response will contain the output of a command similar to `ls`. This will provide a response similar to the following:

```
0000   00 00 00 00 00 b0 b1 40 00 01 00 00 00 ff ff ff   .......@........
0010   ff 01 00 00 00 00 00 00 00 10 01 00 00 00 06 00   ................
0020   00 00 06 02 00 00 00 07 53 75 63 63 65 73 73 0a   ........Success.
0030   09 03 00 00 00 09 04 00 00 00 09 05 00 00 00 09   ................
0040   06 00 00 00 11 03 00 00 00 89 00 00 00 06 07 00   ................
0050   00 00 0c 2f 65 74 63 2f 67 74 6b 2d 32 2e 30 06   .../etc/gtk-2.0.
0060   08 00 00 00 0f 2f 65 74 63 2f 6d 6f 64 70 72 6f   ...../etc/modpro
0070   62 65 2e 64 06 09 00 00 00 0d 2f 65 74 63 2f 6c   be.d....../etc/l
0080   6f 67 63 68 65 63 6b 06 0a 00 00 00 0a 2f 65 74   ogcheck....../et
0090   63 2f 64 63 6f 6e 66 06 0b 00 00 00 08 2f 65 74   c/dconf....../et
00a0   63 2f 76 69 6d 06 0c 00 00 00 0d 2f 65 74 63 2f   c/vim....../etc/
00b0   73 79 73 63 74 6c 2e 64 06 0d 00 00 00 0a 2f 65   sysctl.d....../e
00c0   74 63 2f 72 63 32 2e 64 06 0e 00 00 00 0f 2f 65   tc/rc2.d....../e
00d0   74 63 2f 72 65 73 6f 6c 76 63 6f 6e 66 06 0f 00   tc/resolvconf...
00e0   00 00 0e 2f 65 74 63 2f 77 69 72 65 73 68 61 72   .../etc/wireshar
00f0   6b 06 10 00 00 00 0e 2f 65 74 63 2f 70 72 6f 66   k....../etc/prof
0100   69 6c 65 2e 64 06 11 00 00 00 10 2f 65 74 63 2f   ile.d....../etc/
```

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.