Talos Vulnerability Report

TALOS-2022-1491

Open Automation Software Platform Engine SecureConfigValues denial of service vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26026

Summary

A denial of service vulnerability exists in the OAS Engine SecureConfigValues functionality of Open Automation Software OAS Platform V16.00.0112. A specially-crafted network request can lead to loss of communications. 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:N/I:N/A:H

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 change the port used for configuration changes. If the `SecureConfigValues` command is used to change the `TCP Port` parameter to an invalid value, the OAS Platform will stop listening for new configuration connections altogether. Invalid values consist of any port number outside of the available range (>65535) or any port already in use. 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 successful `SecureConfigValues` command is received, a response similar to the following will be returned:

```
0000   00 00 00 00 00 80 44 40 00 01 00 00 00 ff ff ff   ......D@........
0010   ff 01 00 00 00 00 00 00 00 11 01 00 00 00 02 00   ................
0020   00 00 06 02 00 00 00 07 53 75 63 63 65 73 73 0a   ........Success.
0030   0b                                                .
```

If either an invalid or in-use port was chosen, it will no longer be possible to communicate with the server. If a valid port that was not already in-use was chosen, communication will switch to that port.

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.