Talos Vulnerability Report

TALOS-2022-1513

Open Automation Software OAS Platform REST API unauthenticated vulnerability

MAY 25, 2022

CVE NUMBER

CVE-2022-26833

Summary

An improper authentication vulnerability exists in the REST API functionality of Open Automation Software OAS Platform V16.00.0121. A specially-crafted series of HTTP requests can lead to unauthenticated use of the REST API. An attacker can send a series of HTTP requests to trigger this vulnerability.

Tested Versions

Open Automation Software OAS Platform V16.00.0121

Product URLs

OAS Platform - https://openautomationsoftware.com/knowledge-base/getting-started-with-oas/

CVSSv3 Score

9.4 - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/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.

Included with the platform is a REST API designed to give programmatic access for making configuration changes and viewing data. By default this API ships enabled on port 58725 and supports use of the Default User for a subset of its functionality.

Authentication as the Default User is possible through use of a blank username and password sent to the `authenticate` endpoint with a request similar to the following:

```
POST /OASREST/v2/authenticate HTTP/1.1
Host: ip_addr:58725
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/json
Content-Length: 32

{"username": "", "password": ""}
```

When successful, this request returns a message similar to the following:

```
HTTP/1.1 200 OK
Date: Thu, 07 Apr 2022 18:01:41 GMT
Content-Type: application/json; charset=utf-8
Server: Kestrel
Content-Length: 211
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *

{"status":"OK","data":{"clientid":"e1393f60-9453-4bed-b427-
63ebdb7b0f92","token":"6a4fa444-e42b-4fa1-99f0-f72ddaabcaa7"},"messages":["Default
credential provided - access to data and operations may be limited"]}
```

With valid `clientid` and `token` parameters, it is then possible to make any desired change to the configuration of the platform. Notably the API can be used to perform the following operations:

1. read the existing configuration, usernames, and groups through use of the `options`, `users`, and `security` GET endpoints
2. create a new security group and user with greater permissions than the default user through use of the `users` and `security` POST endpoints
3. change the port on which various OAS services listen through use of the `options` POST endpoint

Mitigation

The easiest way to mitigate attempts to exploit this vulnerability is to create custom Security Groups and User Accounts with only the permissions necessary to complete the needed tasks, and then restrict the access provided by the Default Security Group as much as is allowed. Custom Security Groups and User Accounts can be created through either the OAS Configuration Tool or the REST API. Once custom accounts are successfully created, the Default Security Group should be stripped of all permissions. The easiest way to accomplish this is to use the OAS Configuration Tool by navigating to the `Configure > Security` menu, selecting the `Default` group, selecting `Disable All` for the feature choice, and finally applying the change. When performed successfully this will provide an error any time a request is made as the Default User.

Timeline

2022-04-26 - Vendor Disclosure
2022-05-22 - Vendor Patch Release
2022-05-25 - Public Release

CREDIT

Discovered by Jared Rittle of Cisco Talos.
