Silver Peak Security Advisory

Notification

Issues related to the Silver Peak EdgeConnect web interface

CVE-2019-16100 originally published by the SD-WAN “new hope” team on Sep 8, 2019

CVE ID: CVE-2019-16100 Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows remote attackers to trigger a web-interface outage via slow client-side HTTP traffic from a single source.

Summary

The Silver Peak EdgeConnect Web UI is susceptible to slow HTTP DoS attacks if the web interface is accessible. Silver Peak is evaluating a fix for this.

Recommended Action for Silver Peak Customers

1) Set the EdgeConnect WAN interfaces to harden or stateful firewall mode. This restricts access to the Web UI from anyone outside.
2) Limit Web UI access to IT administrators. This could be done by restricting the access to the Web UI from specified subnets.
3) Optionally, disable direct access to the EdgeConnect Web UI. All functionality remains available through the Orchestrator UI.

   Steps to disable direct access to the EdgeConnect Web UI

   From the Orchestrator, right-click on the appliance name, then click **CLI Session**. In the appliance CLI, enter the following commands at the prompt:

   enable (the prompt changes to #)
   configure terminal
   web http disable
   web https disable
   exit

   Note: To disable access to all appliances at once, use Broadcast CLI from Orchestrator or Orchestrator CLI templates.

   The CLI command is available in EdgeConnect 8.1.9.6 and later.

Applicability to Silver Peak products

Silver Peak product(s)	Applicability
Unity EdgeConnect, NX, VX	Applicable
Unity Orchestrator	Not Applicable
EdgeConnect in AWS, Azure, GCP	Applicable
Silver Peak Cloud Services	Not Applicable

References

The full details of the CVEs can be found at https://www.cvedetails.com/cve/CVE-2019-16100/.

Thank you,
Product Security Incident Response Team at Silver Peak