Silver Peak Security Advisory

Notification

Issues related to the Silver Peak EdgeConnect web interface

CVE-2019-16099, originally published by the SD-WAN "new hope" team on Sep 8, 2019

CVE ID: CVE-2019-16099 Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows CSRF via JSON data to a .swf file.

Summary

The Silver Peak EdgeConnect Web UI does not use anti-CSRF token validation for change requests. Silver Peak is working on adding CSRF token validation for the EdgeConnect Web UI.

Recommended Action for Silver Peak Customers

1) In the appliance Web UI, go to Administration -> Session Management and set Auto Logout to a low value, such as five minutes. This minimizes the window of opportunity for a CSRF attack.
2) 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 CVE can be found at https://www.cvedetails.com/cve/CVE-2019-16099/.

Thank you,
Product Security Incident Response Team at Silver Peak