

Silver Peak Security Advisory

Notification

Issues related to the Silver Peak EdgeConnect web interface

CVE-2019-16104, CVE-2019-16105 originally published by the SD-WAN “new hope” team on Sep 8, 2019

CVE IDs: CVE-2019-16104 Silver Peak EdgeConnect SD-WAN before 8.1.7.x has reflected XSS via the rest/json/configdb/download/ PATH_INFO.

CVE-2019-16105 Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows ..%2f directory traversal via a rest/json/configdb/download/ URI.

Summary

The Silver Peak EdgeConnect Web UI, if accessible, is susceptible to a reflective cross-site scripting (XSS) attack and a directory traversal attack.

Resolution

- XSS fixes were made to 8.1.9.0. Bug ID VXOA-44305 tracks this change.
- Directory traversal fixes were made to 8.1.7.21, 8.1.9.10. Bug ID VXOA-51639 tracks this change.

Recommended Action for Silver Peak Customers

Upgrade to the fixed software versions.

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-2019-16104/> and <https://www.cvedetails.com/cve/CVE-2019-16105/>.

Thank you,
Product Security Incident Response Team at Silver Peak