

# Silver Peak Security Advisory

## Notification

### Issues related to Information Disclosure through Stack Traces

**CVE-2019-16101** originally published by the SD-WAN “new hope” team on Sep 8, 2019

**CVE ID:** CVE-2019-16101 Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows remote attackers to obtain potentially sensitive stack traces by sending incorrect JSON data to the REST API, such as the rest/json/banners URI.

### Summary

An unauthenticated user can send a request containing incorrect JSON to the REST API and get stack trace errors.

### Resolution

This is fixed in Silver Peak EdgeConnect 8.1.9.4 and later.

### Recommended Action for Silver Peak Customers:

Upgrade to 8.1.9.4 or 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-2019-16101/>.

Thank you,  
Product Security Incident Response Team at Silver Peak