Privilege Escalation Vulnerabilities

**CVE-2019-16103 originally published by the SD-WAN “new hope” team on Sep 8, 2019**

**CVE ID:** CVE-2019-16103 Silver Peak EdgeConnect SD-WAN before 8.1.7.x allows privilege escalation (by administrators) from the menu to a root Bash OS shell via the spsshell feature.

**Summary**
By default, Silver Peak EdgeConnect appliances allow an administrator to gain access to the shell. This can be disabled if desired.

**Steps to disable shell access**
If administrators want to disable shell access, they should upgrade to EdgeConnect 8.1.7.0 or later and follow the steps below:

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
- shell disable all
- exit

**Note:** It is an irreversible operation to disable shell access.

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

**Applicability to Silver Peak Products**

<table>
<thead>
<tr>
<th>Silver Peak product(s)</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unity EdgeConnect, NX, VX</td>
<td>Applicable</td>
</tr>
<tr>
<td>Unity Orchestrator</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>EdgeConnect in AWS, Azure, GCP</td>
<td>Applicable</td>
</tr>
<tr>
<td>Silver Peak Cloud Services</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

**References**

Thank you,
Product Security Incident Response Team at Silver Peak