Silver Peak Security Advisory
Notification

Security Advisory 2020-10-31-01-001: Silver Peak Unity Orchestrator™ authentication can be subverted through manipulation of HTTP headers.

CVE ID: CVE-2020-12145
Vulnerability Type: CWE-287: Improper Authentication

Details
Orchestrator uses HTTP headers to authenticate REST API calls from localhost. This makes it possible to log in to Orchestrator by introducing an HTTP HOST header set to 127.0.0.1 or localhost. Orchestrator instances that are hosted by customers – on-premise or in a public cloud provider – are affected by this vulnerability.

Resolution
HTTP headers are no longer used to authenticate localhost REST API calls.

Recommended Actions for Silver Peak Customers
Upgrade to Orchestrator 8.9.11+, 8.10.11+, or 9.0.1+.

Applicability to Silver Peak Products

<table>
<thead>
<tr>
<th>Silver Peak Products</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unity Orchestrator</td>
<td>Applicable</td>
</tr>
<tr>
<td>Unity EdgeConnect, NX, VX</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>EdgeConnect in Public Cloud</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Silver Peak Cloud Services</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Attestation
This vulnerability was reported to Silver Peak by Ariel Tempelhof of Realmode Labs.

References
The full details of the CVE can be found [here](#).

Thank you,
Product Security Incident Response Team at Silver Peak