Silver Peak Security Advisory
Notification

Security Advisory 2020-04-24-01-003: The certificate used to identify the Silver Peak Cloud Portal to EdgeConnect devices is not validated

CVE ID: CVE-2020-12144
Vulnerability Type: CWE-295: Improper Certificate Validation

Details
The certificate used to identify the Silver Peak Cloud Portal to EdgeConnect devices is not validated. This makes it possible for someone to establish a TLS connection from EdgeConnect to an untrusted portal.

Resolution
• Changes have been made to strengthen the initial exchange between EdgeConnect appliances and the Cloud Portal. After the changes, EdgeConnect will validate the certificate used to identify the Silver Peak Cloud Portal to EdgeConnect.

• TLS itself is continually subject to newly discovered and exploitable vulnerabilities. As such, all versions of EdgeConnect software implement additional out-of-band and user-controlled authentication mechanisms.

Recommended Actions for Silver Peak Customers
• Do not change Cloud Portal's IP address as discovered by EdgeConnect appliances.
• Upgrade to Silver Peak Unity ECOS™ 8.3.0.4+ or 8.1.9.12+ and Silver Peak Unity Orchestrator™ 8.9.2+.
• In Orchestrator, enable the “Verify Cloud Portal Certificate” option under Advanced Security Settings.

Applicability to Silver Peak Products

<table>
<thead>
<tr>
<th>Silver Peak Products</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unity EdgeConnect, NX, VX</td>
<td>Applicable</td>
</tr>
<tr>
<td>Unity Orchestrator</td>
<td>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>

Attestation
This vulnerability was reported to Silver Peak by Denis Kolegov, Mariya Nedyak, and Anton Nikolaev from the SD-WAN New Hop team.

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

Thank you,
Product Security Incident Response Team at Silver Peak