Silver Peak Security Advisory

Notification

Security Advisory 2020-04-24-01-002: The certificate used to identify Orchestrator to EdgeConnect devices is not validated

CVE ID: CVE-2020-12143
Vulnerability Type: CWE-295: Improper Certificate Validation

Details

The certificate used to identify Orchestrator to EdgeConnect devices is not validated, which makes it possible for someone to establish a TLS connection from EdgeConnect to an untrusted Orchestrator.

Resolution

- Changes have been made to strengthen the initial exchange between EdgeConnect appliances and the Orchestrator. After the changes, EdgeConnect will validate the certificate used to identify the Orchestrator 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 Orchestrator'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 Orchestrator Certificate" option under Advanced Security Settings and ensure that Orchestrator is not using a self-signed certificate.

Applicability to Silver Peak Products

Silver Peak Products	Applicability
Unity EdgeConnect, NX, VX	Applicable
Unity Orchestrator	Applicable
EdgeConnect in AWS, Azure, GCP	Applicable
Silver Peak Cloud Services	Not Applicable

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