Silver Peak Security Advisory

Notification

Security Advisory 2020-04-24-01-001: IPSec UDP key material can be retrieved from EdgeConnect by a user with admin credentials

CVE ID:	CVE-2020-12142
Vulnerability Type:	CWE-668: Exposure of Resource to Wrong Sphere

Details

IPSec UDP key material can be retrieved from machine-to-machine interfaces and human-accessible interfaces by a user with admin credentials. Such a user, with the required system knowledge, could use this material to decrypt in-flight communication.

The vulnerability requires administrative access and shell access to the EdgeConnect appliance. An admin user can access IPSec seed and nonce parameters using the CLI, REST APIs, and the Linux shell.

Resolution

- EdgeConnect software has been modified to prevent users from accessing IPSec seed and nonce parameters using the CLI, REST APIs, and the Linux shell.

- EdgeConnect software has been modified to allow customers to choose not to persist the IPSec seed for additional security.

Recommended Actions for Silver Peak Customers

Upgrade to Silver Peak Unity ECOS™ 8.3.0.4+ or 8.1.9.12+ and Silver Peak Unity Orchestrator™ 8.9.2+.

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