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

Silver Peak Products	Applicability
Unity Orchestrator	Applicable
Unity EdgeConnect, NX, VX	Not Applicable
EdgeConnect in Public Cloud	Not Applicable
Silver Peak Cloud Services	Not Applicable

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