Silver Peak Security Advisory

Notification

"Authentication bypass in server code - CVE-2018-10933", published by libssh on October 19 2018

Summary:

There is a vulnerability within the server code in libssh 0.6 and later that can cause a client to bypass the authentication process and set the internal state machine maintained by the library to authenticate. As a result, channels are created that are otherwise prohibited.

Silver Peak does not use libssh in any of its products, so this vulnerability does not exist in any Silver Peak deployment scenarios.

Applicability to Silver Peak Deployments: None

This vulnerability is not applicable to

Silver Peak VXOA releases for NX/CPX/EdgeConnect appliances (both physical, virtual, cloud)
Silver Peak Cloud Services - Cloud Orchestrator, Orchestrator^{SP} and Cloud Portal
Silver Peak Orchestrator

Recommended Action for Silver Peak Customers:

None

Resolution:

None

References:

The full details of the advisory and the vulnerabilities are found at:

https://www.libssh.org/security/advisories/CVE-2018-10933.txt

Thank you.

Product Security Incident Response Team

Silver Peak