Silver Peak Security Advisory

Notification

OpenSSL Security Advisory: 22 September 2020

CVE ID: CVE-2020-1968 Raccoon Attack

Summary

The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based cipher suite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH cipher suites and not ECDH cipher suites.

This issue affects OpenSSL 1.0.2, which is out of support and no longer receiving public updates. OpenSSL 1.1.1 is not vulnerable to this issue. Fixed in OpenSSL 1.0.2w (affected in versions 1.0.2-1.0.2v).

Applicability to Silver Peak Products

NOTE: Silver Peak products use OpenSSL for TLS 1.2. However, Silver Peak software is not affected because it does not reuse any DH secrets and does not implement any static DH cipher suites.

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

Recommended Action for Silver Peak Customers

No action is required for Silver Peak customers.

References

Details about this CVE can be found at https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1968.

Thank you,
Product Security Incident Response Team at Silver Peak