Silver Peak Security Advisory

Notification

Silver Peak Products Unaffected by OpenSSL EDIPartyName Vulnerability

Date: 12/17/2020

CVE ID: CVE-2020-1971

Summary

On 12/08/2020, the OpenSSL Software Foundation released a security advisory disclosing the vulnerability described below. The Silver Peak team analyzed the advisory and has concluded that our products are not impacted because they do not utilize the Online Certificate Status Protocol (OSCP) to analyze revoked certificates using CRL.

> The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME. This function behaves incorrectly when both GENERAL_NAME instances contain an EDIPARTYNAME. A NULL pointer de-reference and a crash may occur leading to a possible denial of service attack.
>
> OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes:
>
> 1. Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate
> 2. When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token)

No release of Silver Peak software uses the CRL capability of OpenSSL or the OCSP, so the function is not executed.

Applicability to Silver Peak Products

None.

Recommended Action for Silver Peak Customers

No action is required for Silver Peak customers.

References

Details about this CVE can be found at the following locations:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1971
- https://www.openssl.org/news/secadv/20201208.txt.

Thank you,

Product Security Incident Response Team at Silver Peak