Silver Peak Security Advisory

RFC 5469 compliance

Summary:

DES and IDEA Cipher Suites for Transport Layer Security (TLS) are vulnerable to brute force attack and exhaustive key search attack respectively.

Silver Peak GMS is vulnerable to this vulnerability.

Silver Peak VXOA appliances are susceptible to this vulnerability and patch to resolve the vulnerability is detailed under 'Resolution' heading below.

Details:

RFC 5469 provides information on the advisory and is located at:
https://tools.ietf.org/html/rfc5469

The advisory reads as follows:

4. Security Considerations

4.1. DES Cipher Suites

DES has an effective key strength of 56 bits, which has been known to be vulnerable to practical brute force attacks for over 20 years [DH]. A relatively recent 2006 paper by Kumar, et al. [COPA] describes a system that performs an exhaustive key search in less than nine days on average, and costs less than 10,000 USD to build.

Given this, the single-DES cipher suites SHOULD NOT be implemented by TLS libraries. If a TLS library implements these cipher suites, it

SHOULD NOT enable them by default. Experience has also shown that rarely used code is a source of security and interoperability problems, so existing implementations SHOULD consider removing these cipher suites.

4.2. IDEA Cipher Suite

IDEA has a 128-bit key, and thus is not vulnerable to an exhaustive key search. However, the IDEA cipher suite for TLS has not seen widespread use: most implementations either do not support it, do not enable it by default, or do not negotiate it when other algorithms (such as AES, 3DES, or RC4) are available.

Experience has shown that rarely used code is a source of security and interoperability problems; given this, the IDEA cipher suite SHOULD NOT be implemented by TLS libraries and SHOULD be removed from existing implementations.

Recommended Action for Silver Peak Customers:

Silver Peak GMS (Orchestrator) product:
Silver Peak GMS (Orchestrator) is affected by this vulnerability. It is recommended to upgrade GMS to below mentioned releases to mitigate risk against the vulnerability. The patch is in line with the recommendation in the RFC 5469.

Silver Peak VXOA appliances:
Silver Peak VXOA appliances are affected by this vulnerability. It is recommended to upgrade VXOA appliances to below mentioned releases to address the risk from the vulnerability. The patch is in line with the recommendation in the rfc 5469.

Resolution:

Silver Peak Issue Id 29290 and 29789 tracks this vulnerability.

The Resolution for this vulnerability is in each of the below mentioned branches of release:

VXOA 7.3.4.1 and later releases

VXOA 8.0.1.0 and later releases

VXOA 8.1.0 and later releases

GMS 8.0.1 and later releases

GMS 8.1.0 and later releases