Silver Peak Security Advisory

RC4 algorithm vulnerability to 'plain-text recovery' attacks as used in TLS/SSL

CVE-2013-2566, published by NIST on 03/15/2013

Summary:

US-CERT/NIST advisory for CVE-2013-2566 is dated 03/15/2013. The advisory is about the RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

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:

CVE provides information on the advisory and is located at:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566

The full advisory located at http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566 and reads as follows:

"The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext"

Further NIST guidelines suggest disabling RC4 algorithm for TLS/SSL protocols as a resolution in

http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295, this is detailed under section 3.1.1.1 as below:

3.3.1.1.1 Algorithm Support Many TLS servers and clients support RC4 [Schneier96] cipher suites. RC4 is not an Approved algorithm. If the server were configured to support RC4 cipher suites, they may be chosen over the recommended cipher suites composed of Approved algorithms. Therefore it is important that the server is configured only to use recommended cipher suites. Server implementations may not allow the server administrator to specify preference order. In such servers, the only way to ensure that a server uses Approved algorithms for encryption is to disable cipher suites that use other encryption algorithms (such as RC4 and Camellia [RFC3713]).

NIST has added the vulnerability summary for this CVE to their National Cyber Awareness System database:

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566

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 CVE-2013-2566 advisory.

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 CVE-2013-2566 advisory.

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