ScaleArc: SSL Embedded Certificate Expiration

John DiNapoli - 2016-02-18 - 0 Comments - in Security Advisory & Bulletins

Problem Summary

ScaleArc Support has become aware of an internal SSL Certification expiration issue that can result in some memory leakage under certain circumstances. Please be aware that this issue can impact your environment, and we ask that you contact our support team as soon as possible to avoid any disruption to your production environment. We will also be reaching out to customers whose environments we anticipate might be vulnerable. Please

read on for more details on the issue.

ScaleArc Version Impact

The SSL issue affects all ScaleArc releases – SQL Server, MySQL, Oracle

3.0.x through 3.6.x	Susceptible to memory leak
3.7.x or newer	No memory leak problems but issue needs to be addressed

Solution

DO NOT perform an update of the entire system. Apply an update provided by ScaleArc Support

ScaleArc Support will have a patch and a standard ScaleArc Update Package available. Please contact our 24 x 7 support team via our customer portal at support.scalearc.com or

by email support@scalearc.com to schedule your software update.

Note: During the ScaleArc update, you may need to restart the ScaleArc instance, which

might cause applications to see connection errors and retries.

Additional Details

The issue was identified on Feb 17, 2016

This issue may affect environments where ScaleArc is set up as an Active / Passive High Availability (HA) pair.

The connectivity between the ScaleArc pairs relies on an SSL connection, which requires an embedded SSL certificate. This SSL connection is used to keep the HA pairs in sync on configuration changes and caching among others.

The internal ScaleArc SSL certificate expired on February 11, 2016. As a result, connectivity between the Primary and Secondary ScaleArc instances fails, causing two issues:

When the Primary's SSL connection establishment fails, sync fails, so the Primary is unable to sync any changes to the Secondary

When SSL connection fails, the Primary may experience a memory leak. This leak can eat up memory fast, causing the Primary to slow down and reboot.

The sync between Primary and Secondary ScaleArc instances happens under the following scenarios and will trigger the issues associated with the expired SSL certs:

Initial deployment and setup of ScaleArc, or when an upgrade is done in the customer environment

If Caching is used in existing environments, cache usage and data being processed is sync'd between the two nodes

Any runtime changes of configuration on the Active ScaleArc instance will cause an HA sync

Examples: Cache rules update, configuration changes, and other system updates

If you have any questions specific to ScaleArc appliances, images, or

other deployments, please contact ScaleArc Support directly using

our Support Portal:

Ref: https://wiki.scalearc.com/x/lBgZAw

Permalink:
https://support.scalearc.com/kb/articles/3072

Tags

Expiration

ssl 2016

SSL Certificate

SSL Embedded Certificate Expiration

ssl2016

Attachments

blob [4.87 KB]