Customer Bulletin

Product Model: Archive Appliance
Date: April 2015
Reference ECO number: 369

Reason for Bulletin

A security advisory has been issued by OpenSSH: gcmrekey.adv. The following link is provided for reference: http://www.openssh.com/txt/gcmrekey.adv. In summary, a memory corruption vulnerability exist when an AES-GCM cipher is selected during key exchange. If exploited, this may permit code execution with the privileges of the authenticated user and may allow bypassing restricted shell/command configurations.

Description of Notification

The Archive Management Software running on all of the Archive Appliance and Archive Appliance Express products utilizes the OpenSSH software. More specifically, the OpenSSH version utilized with the AMS 4.20 and prior releases is not affected by this vulnerability, as the issue was introduced with the OpenSSH 6.2 version. Additionally, the AMS 5.0 and higher releases, though utilizing this newer OpenSSH version, do not utilize the particular ciphers which expose the vulnerability. Hence, no action is required in regards to this vulnerability. But, to ensure no usage can occur in the future, these particular ciphers have been disabled from usage via modification of the appropriate configuration file.

We would like to thank you for your diligence regarding the security of your environment, and want to assure you that the resolution of these issues is of the utmost importance to Alliance.

If you require any assistance, please contact Alliance Storage Technologies and speak to one of our support engineers. They will be happy to assist you with any service related questions.