"POODLE" SSL exposure in Dot Hill products
Updated: 2014.11.10

Dot Hill has reviewed all currently released products for the possible exposure of the "POODLE" SSL exploit.

Note that any possible exposure to the "POODLE" exploit on Dot Hill products is limited to the management interface of the product. There is no direct data access exposure from this exploit.

We have found that the following legacy products **are not** exposed to the "POODLE" exploit:

- SANnet Series Products
- 2000 Series (Neptune)
- 2002 Series (Mercury)
- 5000 Series (Krypton)

We have found that the following current shipping products **are** exposed to the "POODLE" exploit:

- 3000 Series (Titanium)
- 4000 Series (Chromium FX)
- 3004/4004 Series (Gallium)

The solution for this exposure is to update to a later version of OpenSSL which contains a fix; the updated version of OpenSSL will be available with the next released of these currently shipping products:

- 3000 Series (Titanium) TS252
- 3004/4004 Series (Gallium) GL205

Once released, the firmware will be available on our Customer Resources Center website: http://crc.dothill.com

Please contact Dot Hill support if you have any questions about this issue.

Email: **support@dothill.com**
Phone: **+1-877-368-7924**
Intl Phone: **001-303-845-3200, option 1**