**“Heartbleed” exposure in Dot Hill products**
**Updated: 2014.04.30**

Upon the announcement of the OpenSSL “Heartbleed” issue, Dot Hill has reviewed all currently released products for the possible exposure of this issue.

Note that any possible exposure to the “Heartbleed” issue on Dot Hill products is limited to the management interface of the product. There is no direct data access exposure from this issue.

We have found that the following products **are not** exposed to the “Heartbleed” issue:

- SANnet Series Products
- 2000 Series (Neptune)
- 2002 Series (Mercury)
- 3000 Series (Titanium) running firmware TS240xxx and earlier
- 3003 Series (Nitro)
- 5000 Series (Krypton)

We have found that the following current shipping products **are** exposed to the “Heartbleed” issue:

- 3000 Series (Titanium) running firmware TS250xxx and later
- 4000 Series (Chromium FX)
- 4004 Series (Gallium)
- Pro 5000 Series (Chromium MX)

Updated Timeline for Patches:

| | |
|---|---|
| • 3000 Series (Titanium) | Mid May ‘14 |
| • 4000 Series (Chromium FX) | Mid May ‘14 |
| • 4004 Series (Gallium) | First week of May ‘14 |
| • Pro 5000 Series (Chromium MX) | End of May ‘14 (included with full patch) |

The patches will be available on our Customer Resources Center website once released: http://crc.dothill.com

Please contact Dot Hill support for the latest updates on progress of the patches.

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