technicolor

Pan Dacom Networking AG
Dreieich Plaza 1B
63303 Dreieich
Deutschland

Issy les Moulineaux, 22 April 2014

Dear Customer,

Last week an important vulnerability referenced CVE-2014-0160 was reported in the press under the popular name “Heartbleed (cf. reference links in the annex).

This letter serves to inform you that none of our DSL products nor software releases for our DSL products have been affected by this Heartbleed OpenSSL bug, since they do not incorporate any of the OpenSSL versions vulnerable to the referenced issue.

If you have further questions, please do not hesitate to contact me or your local Technicolor technical support.

We will make sure to keep you informed in case of further developments.

Kind regards,

Cecile Maiffret

References:

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160&cid=2

http://heartbleed.com/

What OpenSSL versions are affected?

According to the above sources:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

This bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 from 14 March 2012.
OpenSSL 1.0.1g released on 7 April 2014 fixes the bug.