# NOTICE # FN-PRD-PS-Heartbleed-041114-01

| | |
|---|---|
| **Type** | ☐Product Announcement (PA)<br>☑Product Support (PS)<br>☐End of Life (EoL)<br>☐Pricing (PRC)<br>☐Sales & Marketing (S&M)<br>☐Training (T) |
| **Region Applicable** | ☐APAC ☐EMEA ☐NAM ☑All |
| **Subject** | **Heartbleed Security Update** |
| **Field Notice Date** | **April 11, 2014** |
| **Effective Date** | **April 11, 2014** |
| **Notice Number:** | **FN-PRD-PS-Heartbleed-041114-01** |

## Notice

This field notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty, including the warranty of merchantability. Your use of the information on the field notice or materials linked from the field notice is at your own risk. Meru reserves the right to change or update this field notice at any time.

## Summary

OpenSSL "Heartbleed" vulnerability

## Description of Field Notice

This notice is to provide information regarding the Heartbleed vulnerability, how it impacts Meru's products, and what needs to be done to protect your Meru systems from this vulnerability.

Heartbleed Background Information:

CVE-2014-0160 describes a flaw in the heartbeat extension to the SSL protocol. These heartbeats are defined in RFC6520 and used for keep alive messages without the need for renegotiating the SSL session. It is also used for path MTU discovery. This flaw allows attackers to dump up to 64K of memory near the SSL heartbeat on the impacted target. Depending on what's captured at that time, there's potential for obtaining username/password info, and other private keys and data.

This bug was introduced in March 2012 when OpenSSL 1.0.1 was released, and found in subsequent releases up to 1.0.1f. This was patched in OpenSSL 1.0.1g. On the positive side, older versions are not vulnerable.

OpenSSL is used in several ways in Meru products. This includes HTTPS communication in Captive Portal, VPN when used in AP-to-Controller connections, secure RADIUS communication, and SSH/SCP sessions with the controller.

**Affected Products**

- System Director versions 6.0-x, 6.1-0-3

Prior versions of these products used an earlier version of OpenSSL that is not vulnerable. Meru's EzRF Network Management and IDM Guest Access/Device Provisioning applications are not affected.

**Solution**

Meru Networks has fixed the OpenSSL Heartbleed issue in System Director 6.1-1. It is recommended that all customers running prior versions of SD 6.0 or 6.1 upgrade to the latest maintenance release of 6.1-1 when it is generally available, estimated to be on or before April 30.

Customers requiring this fix prior to the release date may request a pre-release version of 6.1-1 from Meru Customer Support which as available now. Please contact Customer Support by opening a ticket at support.merunetworks.com or by calling one of the toll-free support numbers found at www.merunetworks.com