Connect-It and the Heartbleed Vulnerability (CVE-2014-0160)

Revision 1.0

As of: April 18, 2014

Table of Contents

Situation Overview 2

Clarification on the vulnerability applicability 2

- Recommended mitigation plan 2
- Recommended action plan 3

Appendix A 4

- HP Connect-It – Using LDAP or Mail Server 4

Situation Overview

Per the HP Software bulletin, certain versions of the HP Connect-It product were affected by the Heartbleed vulnerability present in the third party OpenSSL library.

Depending on your configuration, you may be impacted (details at the above bulletin and below). Per the bulletin, the following versions of Connect-It include the version of OpenSSL that was found vulnerable. The product versions are:

- Connect-It 9.53 (including all patches)
- Connect-It 9.52 (including all patches)

To remove any doubt, the following Connect-It Product versions were NOT AFFECTED by the Heartbleed vulnerability:

- Connect-It versions: 9.51 (including all patches)
- Connect-It versions: 9.50 (including all patches)
- Connect-It versions: 9.40 (including all patches)
- Connect-It versions: 9.30 (including all patches)

Note: Regardless of the versions listed above, you may still be vulnerable, depending on 3rd party products that are used for the deployment of Connect-It. Please see Appendix A for further details.

HP is not responsible for supporting 3rd party components used to deploy its products and you should treat the guidelines available in Appendix A as recommendations only – for further instructions it is recommended to consult with the 3rd party component vendor.

Clarification on the vulnerability applicability

Some Connect-It connectors can be configured to use OpenSSL to connect to server. The connectors and the connected servers are:

- LDAP connector (LDAP server , OpenLDAP, AD, Novell Directory and IBM)
- POP3 MAIL connector (Mail server like exchange server, hMailserver and etc)
- SMTP MAIL connector (Mail server like exchange server, hMailserver and etc)

Even if using the impacted Connect-It versions and the connectors stated above, your Connect-It deployment is directly impacted only in cases where the Connect-It connectors were configured to use SSL protocol as illustrated in the diagram below:

Connect-It that are not connected to the servers stated above or are connected to the servers stated above using an unsecure connection are not affected by the vulnerability even if using an affected version.

In addition, please take into consideration that in case the Connect-It and the Server are implemented within an organization's intranet, any possible exploit of the vulnerability must result from attacks originating within the network.

Recommended mitigation plan

If your organization's architecture is similar to the above, in order to minimize your exposure to the vulnerability you can take the following action until HP releases a fix to the vulnerability:

Determine the security of the network infrastructure between Connect-It and the Sever. Consider whether implementing one or more proxy servers will mitigate any risks.

Recommended action plan

1. Consult with the vendor of your services servers stated above to confirm whether it uses vulnerable versions of OpenSSL. If so, follow the recommendations from the vendor to fix the vulnerability.
2. Apply a newer version of Connect-It which resolves the vulnerability.

Note: The following are follow-up actions that may be required after the environment has been fully patched:

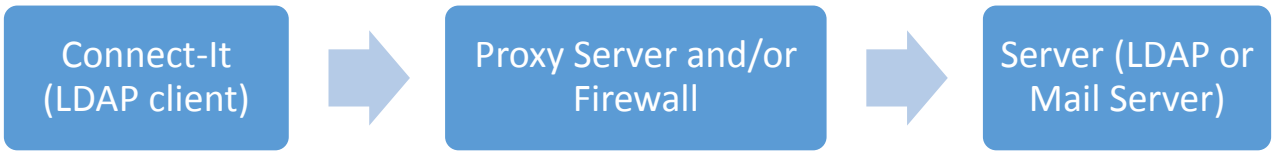
- Generate new keys and certificates for your servers (and proxies as required).
- Generate new SSL certificates for use by the HP Connect-It(s) so that the connection to your servers are functional.
- Change the passwords on your server for all the users used by Connect-It to connect to your server.

The attack vector on Connect-It itself is smaller than that of the server given that Connect-It is acting only as a client. You may search for “reverse heartbleed” for more information.

Appendix A

HP Connect-It – Using LDAP or Mail Server

Organizations where the server is not within the same network as the Connect-It, or that have architectures similar to the following, are also exposed to the vulnerability:



For this scenario, see the action plan above and consider firewall(s), proxy server(s) and the server itself in the action plan.