# Service Manager and the Heartbleed Vulnerability (CVE-2014-0160)

Revision 2

As of: May 8, 2014

# Table of Contents

## Document History

April 15, 2015: Version 1: initial release

May 8, 2014: Version 2: add the "document history" and "patch availability" sections

## Situation Overview

Per the HP Software bulletin, certain versions of the HP Service Manager 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 Service Manager include the version of OpenSSL that was found vulnerable. The product versions are:

- Service Manager 9.32 (including all patches)
- Service Manager 9.33 (GA, 9.33.p1, 9.33.p1-rev1 & 9.33.p2).

To remove any doubt, the following Service Manager Product versions were NOT AFFECTED by the Heartbleed vulnerability:

- Service Manager versions: 9.30, 9.31, 9.20, 9.21, 7.10, 7.11
- ServiceCenter version 6.2

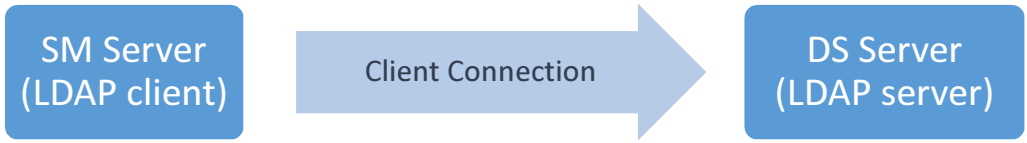
Note: Regardless of the versions listed above, you may still be vulnerable, depending on 3rd party products that are used for the deployment of Service Manager / ServiceCenter. Please see Appendix A for further details.

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

Service Manager Server uses OpenSSL to connect to Directory Services Server via the secure LDAP protocol. Secure LDAP is also known as LDAP over SSL (LDAPS). Examples of Directory Services ("DS") servers are Microsoft Active Directory and Novell eDirectory.

Even if using the impacted Service Manager versions stated above, your Service Manager deployment is directly impacted only in cases where the SM server is integrated with LDAP using Secure LDAP protocol as illustrated in the diagram below:




SM Servers that are not integrated with LDAP or are integrated with LDAP 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 SM Server and the DS 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 SM Server and the DS Sever. Consider whether implementing one or more proxy LDAP severs will mitigate any risks. (For example, if using SM vertical scaling you could implement a non-vulnerable LDAP proxy server on the same physical server as SM to prevent any vulnerable traffic from traversing the network)

**Recommended action plan**

1. Consult with the vendor of your Directory Services server 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 Service Manager 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 Directory Services Server (and proxies as required).
- Generate new SSL certificates for use by the HP Service Manager Server(s) so that the LDAPS integration to your Directory Services Server is functional.
- Generate new passwords for all HP Service Manager users/operators.

The attack vector on Service Manager itself is smaller than that of the Directory Server given that SM is acting only as a client. You may search for “reverse heartbleed” for more information.

## Patch Availability

The following security bulletin outlines the available patches for Service Manager that address this vulnerability:

https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04248997

# Appendix A

## HP Service Manager Server (RTE) – Using LDAP Proxy Server

Organizations where the DS server is not within the same network as the SM server, 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 DS server itself in the action plan.

## HP Service Manager server (RTE) – Load Balancer

In some organizations, a hardware load balancer is deployed in conjunction with multiple SM servers that may leverage OpenSSL to provide HTTPS traffic encryption and load balancing. This is an optional, advanced deployment configuration.

Your hardware load balancer may be impacted if it uses a vulnerable version of OpenSSL. Please see the official vulnerability details for the affected versions, and consult the manufacturer of your device to determine whether you are impacted. If you are using a vulnerable version, you should follow the recommended steps provided by the official vulnerability information and your device manufacturer.

If the hardware load balancer that provides HTTPS for HP SM server is impacted, an attacker could have retrieved SM usernames and passwords as well as any HP SM business data that transits through the hardware load balancer. Please note this is the case for **any** application whose traffic transits through vulnerable servers, and is not specific to HP SM server. It is up to your administrators to take follow-up actions if deemed necessary after patching the issue on your hardware load balancer device(s). Such follow-up actions include the generation new keys on your web server, revocation of old certificates and re-issuance of passwords for all HP SM Server users, etc.

## HP Service Manager web tier, Service Request Catalog, and Mobility

The HP Service Manager web tier does not use OpenSSL and is not directly impacted by the Heartbleed vulnerability. However, it is common in SM Production environments to deploy a web server and/or hardware load balancer device in conjunction with SM web tier servers that may leverage OpenSSL to provide HTTPS traffic encryption.

Although the HP SM web tier is not directly impacted, your web server and hardware load balancer may be impacted if it uses a vulnerable version of OpenSSL. Please see the official vulnerability details for the affected versions and consult with your web server vendor and/or device manufacturer to determine whether you are impacted. If you are using a vulnerable version, you should follow the official steps provided by your web server vendor and/or device manufacturer.

If the web server or hardware load balancer that provides HTTPS for the HP SM web tier is impacted, an attacker could have retrieved SM usernames and passwords as well as any HP SM business data that transits through the Web server. Please note this is the case for **any** application whose traffic transits through vulnerable servers, and is not specific to HP SM web tier. Your administrators should take follow-up actions if deemed necessary after the issue is patched on your web server and/or hardware load balancer device(s). Such follow-up actions include the generation new keys on your web server or hardware load balancer, revocation of old certificates, and re-issuance of passwords for all HP SM Server users, etc.

## HP Service Manager Windows client (Eclipse client)

The HP Service Manager Windows client does not use OpenSSL and is not directly impacted by the Heartbleed vulnerability. However, it is possible in SM production environments to deploy a hardware load balancer device in conjunction with the SM Windows client(s) that may leverage OpenSSL to provide HTTPS traffic encryption.

Although the HP SM Windows client is not directly impacted, your hardware load balancer may be impacted if it uses a vulnerable version of OpenSSL. Please see the official vulnerability details for the affected versions and consult the manufacturer of your

device to see whether you are impacted. If you are using a vulnerable version, you should follow the official steps provided by your device manufacturer.

If the hardware load balancer that provides HTTPS for the HP SM Windows client is impacted, an attacker could have retrieved SM usernames and passwords as well as any HP SM business data that transits through the hardware load balancer. Please note this is the case for **any** application whose traffic transits through vulnerable servers, and is not specific to the HP SM Windows client. Your administrators should take follow-up actions if deemed necessary after patching the issue on your hardware load balancer device(s). Such follow-up actions include the generation new keys on your hardware load balancer, revocation of old certificates, and re-issuance of passwords for all HP SM client users, etc.

## SM Server and KM Search Engine Embedded Tomcat Components

The SM server ships a version of Tomcat that has no HTTPS connectors enabled default. Therefore, out of the box installations are not affected.

However, if you reconfigured or customized the HTTPS connector to use the Apache Portable Runtime or APR (HP does not recommend or document how to do this) you may be impacted. For example, if **both** of the following lines exist in your customized SM server's Tomcat server.xml, you will be affected by the OpenSSL issue:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
<!-- Define a APR SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector protocol="org.apache.coyote.http11.Http11AprProtocol" port="8443" .../>
```

If you have customized the configuration as noted above, the proposed solution is to remove the APR line in server.xml as mentioned below:

1. Navigate to the server .xml file. For the SM Server:

   <SM_Dir>/RUN/tomcat/server.xml

   For the KM Search Engine:

   <KM_SearchEngine_Dir>/tomcat/conf/server.xml

2. Remove or comment out the following line from the file:

   <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="off" />

3. Change HTTPS connectors configuration as follows:

   from
   <Connector protocol="org.apache.coyote.http11.Http11AprProtocol" port="8443" .../>

   to
   <Connector protocol="org.apache.coyote.http11.Http11Protocol" port="8443" .../>

4. Restart Tomcat.
5. Revoke the server certificates that are used in Tomcat and generate new ones.