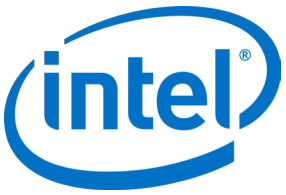
SUPPORT NOTICE
Intel® Enterprise Edition for Lustre* Software
High Performance Data Division



Eliminating the Risk of "POODLE" for Servers Running Intel® EE for Lustre* Software

US
October 23, 2014

Issue

A recently discovered vulnerability in the SSL 3.0 protocol exposes servers to the "man in the middle" information disclosure risk. This specific method of attack is called "Padding Oracle on Downgraded Legacy Encryption" (POODLE). More current security protocols avoid this SSL 3.0 vulnerability, but to support backward compatibility, SSL 3.0 remains a fallback protocol for TLS. Clients may also perform a protocol downgrade to avoid client-server interoperability issues. (For more information about "POODLE," see https://www.openssl.org/~bodo/ssl-poodle.pdf)

This notice describes steps to take to eliminate this specific risk for affected software components included with Intel® Enterprise Edition for Lustre* software.

Affected Software

This risk affects the following software components:

- Intel® Manager for Lustre software
- Hierarchical Storage Management (HSM) software

Intel® Manager for Lustre Software

The risk for Intel® Manager for Lustre software is in the web interface used by the manager GUI and in the communication between the software agents running on Lustre servers and the Intel® EE for Lustre manager software. The agents and the manager GUI both use the same Apache-managed interface on port 443. Accordingly, the resolution is to update the Apache httpd configuration file. This task only needs to be performed on the manager side because the agents on the servers connect outward to the server, and do not accept incoming connections.

Perform the following steps:

1. As root on the server running the Intel® Manager for Lustre software GUI, open the file "/etc/httpd/conf.d/chroma-manager.conf”.

2. Locate the following two lines (which will appear together):

```
SSLProtocol all -SSLv2
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:!LOW:!SSLv2:+EXP
```

3. Change these lines to read:

```
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:!LOW:!SSLv2:!SSLv3:+EXP
```

4. Save the file and restart Intel® Manager for Lustre software using this command:

```
chroma-config restart
```

Restarting Intel® Manager for Lustre software will not affect a running file system, although you must ensure there are no actions, such as starting, formatting, etc., being carried out by the manager software at the time of the restart.

Hierarchical Storage Management Software

For HSM, the vulnerability exists due to HSM’s use of SSL 3.0 in MySQL Server. HSM uses MySQL Server for data storage. Oracle Corporation is the owner of MySQL Server and has released information here:

http://www.oracle.com/technetwork/topics/security/poodlecve-2014-3566-2339408.html

Disclaimer and legal information