



This Technical Advisory describes an issue which may or may not affect the customer's product

# Intel Technical Advisory

TA-1064-1

5200 NE Elam Young Parkway  
Hillsboro, OR 97124

August 29, 2014

## Open SSL vulnerability in Intel® RAID Web Console 2

### Products Affected:

RAID Web Console 2 up to and including version 4.02.01.03

### Description:

OpenSSL.org published a Security Advisory reporting multiple vulnerabilities in OpenSSL. The majority of these are a new set of vulnerabilities following additional scrutiny on the OpenSSL code after the "HeartBleed" issue was identified.

Product/Service Name	Affected Version(s)	Affected by which OpenSSL CVE number(s)
RAID Web Console 2	Up to and including v4.02.01.03	CVE-2014-0224, CVE-2014-0221, CVE-2014-0195, CVE-2014-3470, CVE-2014-0076

### Root Cause:

An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.

Details for the listed Common Vulnerabilities and Exposures (CVE)s:

#### **CVE-2014-0224**

The attack can only be performed between a vulnerable client \*and\* server. OpenSSL clients are vulnerable in all versions of OpenSSL.

#### **CVE-2014-0221**

By sending an invalid DTLS handshake to an OpenSSL DTLS client the code can be made to recurse eventual crash in a DoS attack.

#### **CVE-2014-0195**

This is potentially exploitable to run arbitrary code on a vulnerable client or server.

#### **CVE-2014-3470**

TLS clients enabling anonymous ECDH ciphersuites are subject to a denial of service attack.

#### **CVE-2014-0076**

Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack.

## Corrective Action / Resolution:

The corrective action consists of two parts.

- OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
- OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.  
and
- RAID Web Console 2 should be upgraded to version [14.05.02.03](#) or later available in September 2014.

Please contact your Intel Sales Representative if you require more specific information about this issue.

*INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.*

*A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.*

*Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.*

*The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.*

Intel Corporation