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.

Intel Corporation