hard.

***CVE-2014-3569 Impact analysis on WR SSL and test approach***

**Prepared For RICOH**

**CONFIDENTIAL**

Version: 1.00

Date: May 8, 2015

Version: 1.00

Date:

Wind River Systems, Inc.

9855 Scranton Road, Building 5

San Diego, CA 92121

858-824-3100 phone

858-824-3198 fax

[www.windriver.com](http://www.windriver.com)

Copyright

Unless otherwise agreed in writing, all copyright and intellectual property rights embodied in this document are and shall remain the property of Wind River Systems, Inc. This document is provided solely for the purposes of evaluating the work proposed and no other rights whatsoever to use the information herein are granted. The contents of this document may not be disclosed to any third party without the prior written consent of Wind River Systems, Inc.

Trademarks

Wind River, the Wind River logo, Tornado, and VxWorks are registered trademarks of Wind River Systems, Inc. Any third party trademarks referenced are the property of their respective owners. For further information regarding Wind River trademarks, please see <http://www.windriver.com/company/terms/trademark.html>.

| Revision History | | | |
| --- | --- | --- | --- |
| Date | Version | By | Description of Change |
| May 8, 2015 | 1.00 | Wind River | Official Release. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 5](#_Toc418850911)

[1.1 Purpose and Scope 5](#_Toc418850912)

[1.2 Applicable Documents 5](#_Toc418850913)

[1.3 Glossary 5](#_Toc418850914)

[2 Impact analysis and Test Approach 6](#_Toc418850915)

[2.1 Vulnerability Summary 6](#_Toc418850916)

[2.2 Details of Vulnerability & Method of Exploit 6](#_Toc418850917)

[2.2.1 Background 6](#_Toc418850918)

[2.2.2 Method of Exploit 6](#_Toc418850919)

[2.3 Implementation Behavior – OpenSSL & Wind River SSL 7](#_Toc418850920)

[2.3.1 OpenSSL 0.9.8zc 7](#_Toc418850921)

[2.3.2 OpenSSL 0.9.8zd 8](#_Toc418850922)

[2.3.3 Wind River – SSL 8](#_Toc418850923)

[2.3.4 Required Actions on WR-SSL 8](#_Toc418850924)

[2.3.5 Test Approach 9](#_Toc418850925)

[2.4 Summary/Conclusion 9](#_Toc418850926)

[2.5 Attachments 9](#_Toc418850927)

# Overview

## Purpose and Scope

The Purpose of this Document is to explain details of impact analysis carried out on Wind River SSL stack used RICOH for security vulnerabilities as described in CVE-2014-3569.

Document also includes details of fix released by OpenSSL community, applicability and methods of test and verification of same under Wind River SSL.

## Applicable Documents

The following documents are referenced within:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Document | Version | Scope |
| 1 | CVE-2014-3569\_Test\_Report1 | 0.01 | Test results for WR-SSL server with OPENSSL\_NO\_SSL3 flags set, without patch applied  and  OpenSSL client with –ssl3 option |
| 2 | CVE-2014-3569\_Test\_Report2 | 0.01 | Test results for WR-SSL server with OPENSSL\_NO\_SSL3 flags set, with patch applied  and  OpenSSL client with –ssl3 option |
|  |  |  |  |

## Glossary

|  |  |
| --- | --- |
| Term | Definition |
| WR | Wind River |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
|  |  |
|  |  |

# Impact analysis and Test Approach

## Vulnerability Summary

CVE-2014-3569 is security vulnerability discovered in the OpenSSL implementation in Jan 2015 timeframe.

Security threat uncovered is that OpenSSL server with fix for CVE-2014-3568 applied, results in NULL pointer dereference when a client tries to connect to the server using SSLv3 protocol. This happens only if fix for CVE-2014-3568 was applied.

CVE-2014-3568 is that OpenSSL server with SSLv3 disabled using build flag, still accepts connection when a client tries to connect to the server using SSLv3 protocol.

Details of the vulnerability are described in following section.

## Details of Vulnerability & Method of Exploit

### Background

CVE-2014-3568:

OpenSSL server with SSLv3 disabled using build flag, still accepts connection when a client tries to connect to the server using SSLv3 protocol.

CVE-2014-3569:

OpenSSL server with fix for CVE-2014-3568 applied, results in NULL pointer dereference when a client tries to connect to the server using SSLv3 protocol. This happens only if fix for CVE-2014-3568 was applied.

### Method of Exploit

OpenSSL clients can force OpenSSL server with CVE-2014-3568 vulnerability to use SSL3.0 protocol though it was disabled by build. This is done by client specifying that it can support only SSl3.0. This exposes server to various vulnerabilities existing in SSL3.0 for which patches may not have been applied as SSL3.0 is intended to be disabled at build time and never used.

OpenSSL clients can do denial or service attack on OpenSSL server with CVE-2014-3569 vulnerability. This is done by client specifying that it can support only SSl3.0 that results in server trying to use SSl3.0 which in turn sets the s->method to NULL pointer. A dereference of this NULL pointer can cause server to exit abnormal.

## Implementation Behavior – OpenSSL & Wind River SSL

### OpenSSL 0.9.8zc

There are two ways of disabling SSLv3 support in WR-SSL.

* Disable SSLv3 during build-time by setting OPENSSL\_NO\_SSL3 build flag.
* Disable SSlv3 support be adding a command line argument to the server or client application (*e.g. openssl s\_client –no-ssl3 …*)

Vulnerability CVE-2014-3568 is applicable to OpnSSL 0.9.8zb when built with OPENSSL\_NO\_SSL3 build flag.

OpenSSL 0.9.8zb version, acting as SSL server, sets the server method to SSLv23\_server\_method during startup and listens to client connection requests by invoking function ssl23\_accept() function. (The function ssl23\_accept() is set to the “ssl\_accept” field of SSLxx\_server\_data structure). The function ssl23\_accept(), after receiving ClientHello, invokes, ssl23\_get\_client\_hello() function. Server checks the version requested by client and if SSL3 is the version requested, s->method is set to SSLv3\_server\_method(). After this it proceeds to establish the connection. However since SSL3 was disabled by build option, s->method should not have been set to SSLv3\_server\_method. This behavior can be exploited by a client to force SSLv3 connection even when SSLv3 is disabled build time.

Fix for CVE-2014-3568 is applied to version 0.9.8zc. These code changes introduce a new condition check before s->method is assigned. The code change is as given below.

ssl/ssl23\_srvr.c

559 if ((type == 2) || (type == 3))

560 {

561 /\* we have SSLv3/TLSv1 (type 2: SSL2 style, type 3: SSL3/TLS style) \*/

562 s->method = ssl23\_get\_server\_method(s->version);

563 if (s->method == NULL)

564 {

565 SSLerr(SSL\_F\_SSL23\_GET\_CLIENT\_HELLO,SSL\_R\_UNSUPPORTED\_PROTOCOL);

566 goto err;

567 }

Above code checks if client requested SSLv3 and if so, invokes function ssl23\_get\_server\_method() with s->version as argument. This function internally checks if the SSLv3 is actually enabled by the build flag OPENSSL\_NO\_SSL3 and if not returns NULL. Hence s->method will be set to NULL and connection attempt fails.

However since CVE-2014-3568 fix sets s->method to NULL, it introduced another vulnerability that is described in CVE-2014-3569. This vulnerability is that since the s->method is set to NULL, a SSL client can try to make SSL server use SSLv3 and thus set s->method to NULL which may later result in a NULL pointer dereference.

### OpenSSL 0.9.8zd

Code changes to fix vulnerability of s->method being set to NULL (CVE-2014-3569) is introduced in OpenSSL\_0\_9\_8zd and is as shown below.

ssl/ssl23\_srvr.c

559 if ((type == 2) || (type == 3))

560 {

561 /\* we have SSLv3/TLSv1 (type 2: SSL2 style, type 3: SSL3/TLS style) \*/

562 SSL\_METHOD \*new\_method;

563 new\_method = ssl23\_get\_server\_method(s->version);

564 if (new\_method == NULL)

565 {

566 SSLerr(SSL\_F\_SSL23\_GET\_CLIENT\_HELLO,SSL\_R\_UNSUPPORTED\_PROTOCOL);

567 goto err;

568 }

569 s->method = new\_method;

Above fix uses a new variable new\_method that will invoke ssl23\_get\_server\_method () and may be set to NULL if SSLv3 was disabled at build time. However after the function invocation the variable new\_method is checked for NULL and connection is aborted. If not NULL the value is assigned to s->method and handshake proceeds normally.

### Wind River – SSL

WR-SSL code changes are similar to OpenSSL 0.9.8zc as explained in section 2.3.1. However, WR-SSL server application, during startup, selects a server method as shown below.

500 #if !defined(OPENSSL\_NO\_SSL2) && !defined(OPENSSL\_NO\_SSL3)

501 meth=SSLv23\_server\_method();

502 #elif !defined(OPENSSL\_NO\_SSL3)

503 meth=SSLv3\_server\_method();

504 #elif !defined(OPENSSL\_NO\_SSL2)

505 meth=SSLv2\_server\_method();

506 #endif

Hence when OPENSSL\_NO\_SSL3 is defined, meth will be set to SSLv2\_server\_method(). This way WR-SSL application does not invoke any of the SSLv23\_xxxx functions including ssl23\_accept and ssl23\_get\_client\_hello. Hence the vulnerability as explained above for CVE-2014-3568 (and hence CVE-2014-3569) are not applicable.

However as there could be another application that acts as server of client which can set the method to SSLv23\_server\_method, as WR-SSL stack it is still vulnerable.

### Required Actions on WR-SSL

Following code changes are required for WR-SSL.

ssl/ssl23\_srvr.c

        if ((type == 2) || (type == 3))

                {

                /\* we have SSLv3/TLSv1 (type 2: SSL2 style, type 3: SSL3/TLS style) \*/

+               const SSL\_METHOD \*new\_method;

+               new\_method = ssl23\_get\_server\_method(s->version);

+               if (new\_method == NULL)

+                        {

+                        SSLerr(SSL\_F\_SSL23\_GET\_CLIENT\_HELLO,SSL\_R\_UNSUPPORTED\_PROTOCOL);

+                       goto err;

+                        }

+               s->method = new\_method;

                if (!ssl\_init\_wbio\_buffer(s,1)) goto err;

[Refer to Section 2.3.2 for explanation]

### Test Approach

1. Modify WR-SSL server to set the server method to SSLv23\_server\_method.
2. Connect using OpenSSL client with –sslv3 option
3. Client should be able to establish connection successfully as WR-SSL server is vulnerable. (Report1)
4. Apply patch for CVE-2014-3568 and CVE-2014-3569 to ssl/ssl23\_srvr.c and rebuild VxWorks
5. Repeat steps 1 and 2.
6. SSL client shall fail to establish connection. This indicates that server is no longer vulnerable after applying patch. (Report 2)

## Summary/Conclusion

Detailed examination of the WR-SSL implementation reveals that WR-SSL is vulnerable to the security issue described in CVE-2014-3568 though SSL server application included as part of WR-SSL package is not vulnerable. As CVE-2014-3569 vulnerability is applicable only if CVE-2014-3568 is applicable, WR-SSL is vulnerable to CVE-2014-3569.

Required code changes were made and tests performed.

## Attachments

1. Report1 test results for WR-SSL server without patch applied and OpenSSL client with –ssl3 option
2. Report2 test results for WR-SSL server with patch applied and OpenSSL client with –ssl3 option

/EOD