hard.

***CVE-2015-1789 Impact analysis on WR SSL and test approach***

**Prepared For RICOH**

**CONFIDENTIAL**

Version:

Date:

Version:

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 |
| Aug 20, 2015 | 0.01 | NM team | First Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 5](#_Toc428456856)

[1.1 Purpose and Scope 5](#_Toc428456857)

[1.2 Applicable Documents 5](#_Toc428456858)

[1.3 Glossary 5](#_Toc428456859)

[2 Impact analysis and Test Approach 6](#_Toc428456860)

[2.1 Vulnerability Summary 6](#_Toc428456861)

[2.2 Details of Vulnerability & Method of Exploit 6](#_Toc428456862)

[2.2.1 Background 6](#_Toc428456863)

[2.2.2 Method of Exploit 7](#_Toc428456864)

[2.3 Implementation Behavior – OpenSSL & Wind River SSL 7](#_Toc428456865)

[2.3.1 OpenSSL 0.9.8zf 7](#_Toc428456866)

[2.3.2 OpenSSL 0.9.8zg 8](#_Toc428456867)

[2.3.3 Wind River – SSL 9](#_Toc428456868)

[2.3.4 Required Actions on WR-SSL 9](#_Toc428456869)

[2.3.5 Test Approach 9](#_Toc428456870)

[2.4 Summary/Conclusion 10](#_Toc428456871)

[2.5 Attachments 10](#_Toc428456872)

# 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-2015-1789.

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-2015-1789\_Test\_Report1 | 0.01 | Report1: test results for WR-SSL as server WITHOUT Fix, OpenSSL 1.0.1 as client, CRAFTED client certificate |
| 2 | CVE-2015-1789\_Test\_Report2 | 0.01 | Report2: test results for WR-SSL as server WITH Fix, OpenSSL 1.0.1 as client, CRAFTED client certificate |
| 3 | CVE-2015-1789\_Test\_Report3 | 0.01 | Report 3: test results for WR-SSL as server WITH Fix, OpenSSL 1.0.1 as client, NOT CRAFTED (good) client certificate |
|  |  |  |  |

## Glossary

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

# Impact analysis and Test Approach

## Vulnerability Summary

CVE-2015-1789 is security vulnerability discovered in the OpenSSL implementation in June 2015 timeframe.

Security threat uncovered is that the X509\_cmp\_time function in crypto/x509/x509\_vfy.c in OpenSSL before 0.9.8zg in 0.9.8 branch, before 1.0.0s in 1.0.0 branch, 1.0.1 before 1.0.1n in 1.0.1 branch, and before 1.0.2b in 1.0.2 branch allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1\_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback

Details of the vulnerability are described in following section.

## Details of Vulnerability & Method of Exploit

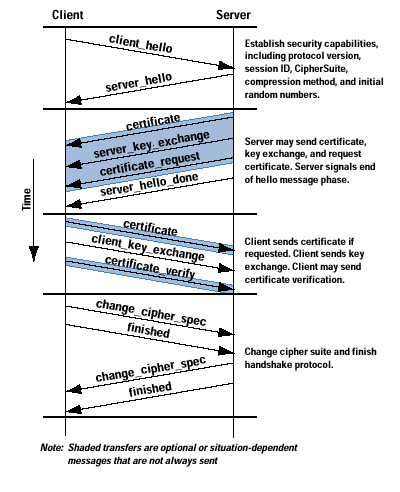
### Background

OpenSSL server application that supports client authentication with custom verification callback may be forced to out-of-bound memory access and possible crash if X509 certificate with crafted time length and values are given as input.

SSL protocol allows server to request a client to furnish its certificate to authenticate the client. In such a scenario, server sends a certificate request and client responds with a certificate message that contains its certificate.

Following diagram illustrates the message exchanges.

[ <http://qwefgh90.github.io/_images/sslhand.gif> ]



In case of server, a client verification call back if set by function, SSL\_CTX\_set\_verify(), will be invoked at the time server receives a “Certificate” message from client. All client certificates shall be available to server application through argument to above callback function. Callback function can make use of various OpenSSL functions to inspect contents of the certificate and perform verification.

Applications that perform verification of validity of certificates need to work with two time values that is part of X.509 certificates namely notBefore and notAfter. These values are of type ASN1\_STRING that includes a type, length and value. WR\_SSL provides a function X509\_cmp\_time() to compare the time in ASN1\_STRING form to the time value in a time\_t structure.

### Method of Exploit

Assume a WR-SSL server application that will perform client verification using a callback function. As explained in above section, the callback will be invoked with client certificate details.

A remote attacker can exploit above behavior by creating a crafted certificate and using that certificate as client certificate. Certificate validity is expressed using two timestamp values that can be of following formats. (Assuming UTCTIME)

**UTCTIME**

YYMMDDHHMMZ

YYMMDDHHMMSSZ

YYMMDDHHMMSS+hhmm

When encoded in TV format, the above values shall be of minimum length 11 and maximum 17 octets.

As example, attacker can manipulate the time information as below –

Create a timestamp with length as 17 but content as 1504102155-ÓZ . While the length is correct, the character after ‘-‘ (marked in RED) is junk and overall value falls short of 17 bytes.

However the current WR-SSL implementation of X509\_cmp\_time() function does not handle such a case safely and result in out-of-bound access. Details of implementation are explained in next section.

## Implementation Behavior – OpenSSL & Wind River SSL

### OpenSSL 0.9.8zf

Implementation of X509\_cmp\_time() in ~/crypto/x509/x509\_vfy.c is explained below:

Potential out of bound cases are marked.

The function takes a ASN1\_TIME structure and time\_t structure as input.

|  |  |
| --- | --- |
| Code blocks (not continuous) | Description/Analysis |
| i=ctm->length;  str=(char \*)ctm->data; | Variable I is the length of time string  Timestring part of ctm is copied to str. |
| if ((i < 11) || (i > 17)) return 0; | Time string can be foll formats  YYMMDDHHMMZ  YYMMDDHHMMSSZ  YYMMDDHHMMSS+hhmm  Hence min is 11 and max is 17. Good validity check |
| /\* Skip any fractional seconds... \*/  if (\*str == '.') {  while ((\*str >= '0') && (\*str <= '9')) str++; | No checks in while loop  Potential out of bound access |
| if ((\*str != '+') && (str != '-'))  return 0;  offset=((str[1]-'0')\*10+(str[2]-'0'))\*60;  offset+=(str[3]-'0')\*10+(str[4]-'0'); | No prior check for str[1] through str[4]  Potential out of bound access |

### OpenSSL 0.9.8zg

Revision to function X509\_cmp\_time() in ~/crypto/x509/x509\_vfy.c to fix CVE-2015-1789 vulnerability introduces many strict format and buffer overflow checks. Few of the changes are listed below.

|  |  |
| --- | --- |
| Code blocks (not continuous) | Description/Analysis |
| remaining = ctm->length;  **str=(char \*)ctm->data;** | New variable “remaining” to keep track of remaining bytes to check |
| int min\_length = sizeof("YYYYMMDDHHMMZ") - 1;  **int max\_length = sizeof("YYYYMMDDHHMMSS.fff+hhmm") - 1;**  **if (remaining < min\_length || remaining > max\_length)**  **return 0;** | Stronger length check including maximum |
| if (remaining && \*str == '.') {  str++;  remaining--;  for (i = 0; i < 3 && remaining; i++, str++, remaining--) {  if (\*str < '0' || \*str > '9')  break;  }  } | Stronger bound check than the while loop earlier |
| if ((\*str != '+') && (\*str != '-'))  return 0;  /\* Historical behaviour: the (+-)hhmm offset is forbidden in RFC5280. \*/  if (remaining != 5) return 0;  if (str[1] < '0' || str[1] > '9' ||  str[2] < '0' || str[2] > '9' ||  str[3] < '0' || str[3] > '9' ||  str[4] < '0' || str[4] > '9')  return 0;  offset=((str[1]-'0')\*10+(str[2]-'0'))\*60;  offset+=(str[3]-'0')\*10+(str[4]-'0'); | Stronger check for out-of-bound access. |

### Wind River – SSL

For this CVE, relevant part of WR-SSL implementation is same OpenSSL 0.9.8zg.

Hence all changes made by OpenSSL team to fix the CVE are applicable to WR-SSL as well.

### Required Actions on WR-SSL

Required code changes for WR-SSL are same as those changed between OpenSSL0.9.8zf nad OpenSSL0.9.8zg. See section 2.3.2 for an outline of major changes.

### Test Approach

**Test Scenario 1 (Report 1):**

* Perform connection Test: WR-SSL as server WITHOUT Fix, OpenSSL 1.0.1 as client, CRAFTED client certificate
* Expected Result – Server console should print “OUT OF BOUND ACCESS” error message

**Test Scenario 2 (Report 2):**

* Perform connection Test : WR-SSL as server WITH Fix, OpenSSL 1.0.1 as client, CRAFTED client certificate
* Expected Result – Server console should NOT print “OUT OF BOUND ACCESS” error message

**Test Scenario 3 (Report 3):**

* Perform connection Test: WR-SSL as server WITH Fix, OpenSSL 1.0.1 as client, NOT CRAFTED (good) client certificate
* Expected Result – Server console should NOT print “OUT OF BOUND ACCESS” error message, connection and disconnection should succeed.

## Summary/Conclusion

Detailed examination of the WR-SSL implementation reveals that WR-SSL is vulnerable to the security issue described in CVE-2015-1789.

Required code changes were made and tests performed.

## Attachments

1. Report1: test results for WR-SSL as server WITHOUT Fix, OpenSSL 1.0.1 as client, CRAFTED client certificate
2. Report2: test results for WR-SSL as server WITH Fix, OpenSSL 1.0.1 as client, CRAFTED client certificate
3. Report 3: test results for WR-SSL as server WITH Fix, OpenSSL 1.0.1 as client, NOT CRAFTED (good) client certificate

/EOD