VASCO Security Advisory

Multiple OpenSSL vulnerabilities in VASCO products

Advisory ID: vasco-sa-20150413-openssl

Revision number: 1.0

Date and time of release: April 13 2015 12:00 UTC

Date and time of last update: April 13 2015 12:00 UTC

Summary

On March 19, 2015, the OpenSSL Project published a security advisory describing fourteen vulnerabilities in the OpenSSL library. The vulnerabilities are referred to as follows:

- OpenSSL 1.0.2 ClientHello sigalgs DoS (CVE-2015-0291)
- Reclassified: RSA silently downgrades to EXPORT_RSA [Client] (CVE-2015-0204)
- Multiblock corrupted pointer (CVE-2015-0290)
- Segmentation fault in DTLSv1_listen (CVE-2015-0207)
- Segmentation fault in ASN1_TYPE_cmp (CVE-2015-0286)
- Segmentation fault for invalid PSS parameters (CVE-2015-0208)
- ASN.1 structure reuse memory corruption (CVE-2015-0287)
- PKCS7 NULL pointer dereferences (CVE-2015-0289)
- Base64 decode (CVE-2015-0292)
- DoS via reachable assert in SSLv2 servers (CVE-2015-0293)
- Empty CKE with client auth and DHE (CVE-2015-1787)
- Handshake with unseeded PRNG (CVE-2015-0285)
- Use After Free following d2i_ECPrivatekey error (CVE-2015-0209)
- X509_to_X509_REQ NULL pointer deref (CVE-2015-0288)

Multiple VASCO products incorporate a version of the OpenSSL library affected by one or more vulnerabilities that could allow an unauthenticated, remote attacker to perform a man-in-the-middle attack, inject SSL/TLS session data or disrupt the availability of a service.

Impacted products

The following products are affected by one or more of the above mentioned vulnerabilities:

- IDENTIKEY Federation Server 1.4, 1.5
- IDENTIKEY Authentication Server 3.4 SR1, 3.5, 3.6
- All supported versions of IDENTIKEY (Virtual) Appliance
- aXsGUARD Gatekeeper 7.7.x, 8.0.0, 8.1.0

Detailed description of vulnerability

The following vulnerability descriptions are extracted from the OpenSSL security advisory.

OpenSSL 1.0.2 ClientHello sigalgs DoS (CVE-2015-0291)

If a client connects to an OpenSSL 1.0.2 server and renegotiates with an invalid signature algorithms extension a NULL pointer dereference will occur. This can be exploited in a DoS attack against the server.

Reclassified: RSA silently downgrades to EXPORT_RSA [Client] (CVE-2015-0204)

This security issue was previously announced by the OpenSSL project and classified as "low" severity. This severity rating has now been changed to "high".

This was classified low because it was originally thought that server RSA export ciphersuite support was rare: a client was only vulnerable to a MITM attack against a server which supports an RSA export ciphersuite. Recent studies have shown that RSA export ciphersuites support is far more common.

Multiblock corrupted pointer (CVE-2015-0290)

OpenSSL 1.0.2 introduced the "multiblock" performance improvement. This feature only applies on 64 bit x86 architecture platforms that support AES NI instructions. A defect in the implementation of "multiblock" can cause OpenSSL's internal write buffer to become incorrectly set to NULL when using non-blocking IO. Typically, when the user application is using a socket BIO for writing, this will only result in a failed connection. However if some other BIO is used then it is likely that a segmentation fault will be triggered, thus enabling a potential DoS attack.

Segmentation fault in DTLSv1_listen (CVE-2015-0207)

The DTLSv1_listen function is intended to be stateless and processes the initial ClientHello from many peers. It is common for user code to loop over the call to DTLSv1_listen until a valid ClientHello is received with an associated cookie. A defect in the implementation of DTLSv1_listen means that state is preserved in the SSL object from one invocation to the next that can lead to a segmentation fault. Errors processing the initial ClientHello can trigger this scenario. An example of such an error could be that a DTLS1.0 only client is attempting to connect to a DTLS1.2 only server.

Segmentation fault in ASN1_TYPE_cmp (CVE-2015-0286)

The function ASN1_TYPE_cmp will crash with an invalid read if an attempt is made to compare ASN.1 boolean types. Since ASN1_TYPE_cmp is used to check certificate signature algorithm consistency this can be used to crash any certificate verification operation and exploited in a DoS attack. Any application which performs certificate verification is vulnerable including OpenSSL clients and servers which enable client authentication.

Segmentation fault for invalid PSS parameters (CVE-2015-0208)

The signature verification routines will crash with a NULL pointer dereference if presented with an ASN.1 signature using the RSA PSS algorithm and invalid parameters. Since these routines are used to verify certificate signature algorithms this can be used to crash any certificate verification operation and exploited in a DoS attack. Any application which performs certificate verification is vulnerable including OpenSSL clients and servers which enable client authentication.

ASN.1 structure reuse memory corruption (CVE-2015-0287)

Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Such reuse is and has been strongly discouraged and is believed to be rare.

Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected. Certificate parsing (d2i_X509 and related functions) are however not affected. OpenSSL clients and servers are not affected.

PKCS7 NULL pointer dereferences (CVE-2015-0289)

The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

Applications that verify PKCS#7 signatures, decrypt PKCS#7 data or otherwise parse PKCS#7 structures from untrusted sources are affected. OpenSSL clients and servers are not affected.

Base64 decode (CVE-2015-0292)

A vulnerability existed in previous versions of OpenSSL related to the processing of base64 encoded data. Any code path that reads base64 data from an untrusted source could be affected (such as the PEM processing routines).

Maliciously crafted base 64 data could trigger a segmentation fault or memory corruption. This was addressed in previous versions of OpenSSL but has not been included in any security advisory until now.

DoS via reachable assert in SSLv2 servers (CVE-2015-0293)

A malicious client can trigger an OPENSSL_assert (i.e., an abort) in servers that both support SSLv2 and enable export cipher suites by sending a specially crafted SSLv2 CLIENT-MASTER-KEY message.

Empty CKE with client auth and DHE (CVE-2015-1787)

If client auth is used then a server can seg fault in the event of a DHE ciphersuite being selected and a zero length ClientKeyExchange message being sent by the client. This could be exploited in a DoS attack.

Handshake with unseeded PRNG (CVE-2015-0285)

Under certain conditions an OpenSSL 1.0.2 client can complete a handshake with an unseeded PRNG. The conditions are:

- The client is on a platform where the PRNG has not been seeded automatically, and the user has not seeded manually
- A protocol specific client method version has been used (i.e. not SSL_client_methodv23)
- A ciphersuite is used that does not require additional random data from the PRNG beyond the initial ClientHello client random (e.g. PSK-RC4-SHA).

If the handshake succeeds then the client random that has been used will have been generated from a PRNG with insufficient entropy and therefore the output may be predictable.

Use After Free following d2i_ECPrivatekey error (CVE-2015-0209)

A malformed EC private key file consumed via the d2i_ECPrivateKey function could cause a use after free condition. This, in turn, could cause a double free in several private key parsing functions (such as d2i_PrivateKey or EVP_PKCS82PKEY) and could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources. This scenario is considered rare.

X509_to_X509_REQ NULL pointer deref (CVE-2015-0288)

The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid. This function is rarely used in practice.

Severity score

The tables below denote the CVSS 2.0 vulnerability score of the various vulnerabilities.

OpenSSL 1.0.2 ClientHello sigalgs DoS (CVE-2015-0291)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

RSA silently downgrades to EXPORT_RSA [Client] (CVE-2015-0204)

CVSS Base Score: 4.3					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None required	None	Partial	None

Multiblock corrupted pointer (CVE-2015-0290)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

Segmentation fault in DTLSv1_listen (CVE-2015-0207)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

Segmentation fault in ASN1_TYPE_cmp (CVE-2015-0286)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

Segmentation fault for invalid PSS parameters (CVE-2015-0208)

CVSS Base Score: 4.3

Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None required	None	None	Partial

ASN.1 structure reuse memory corruption (CVE-2015-0287)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

PKCS7 NULL pointer dereferences (CVE-2015-0289)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

Base64 decode (CVE-2015-0292)

CVSS Base Score: 7.5					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	Partial	Partial	Partial

DoS via reachable assert in SSLv2 servers (CVE-2015-0293)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

Empty CKE with client auth and DHE (CVE-2015-1787)

CVSS Base Score: 2.6					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	High	None required	None	None	Partial

Handshake with unseeded PRNG (CVE-2015-0285)

CVSS Base Score: 4.3					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None required	Partial	None	None

Use After Free following d2i_ECPrivatekey error (CVE-2015-0209)

CVSS Base Score: 6.8					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None required	Partial	Partial	Partial

X509_to_X509_REQ NULL pointer deref (CVE-2015-0288)

CVSS Base Score: 5.0					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None required	None	None	Partial

Product fixes and workarounds

VASCO will fix these vulnerabilities in the upcoming releases of the following server-side products:

- IDENTIKEY Appliance 3.8.9.0
- IDENTIKEY Authentication Server 3.8
- IDENTIKEY Federation Server 1.6
- aXsGUARD Gatekeeper 8.2

Obtaining product releases with fixes

- For aXsGUARD Gatekeeper products:

  VASCO will deploy patches via the automated update service. Customers that do not allow their system to receive updates via this service should contact VASCO for instructions about how to obtain the patch.

- For other products

  Customers with a maintenance contract can obtain fixed product releases from MyMaintenance. Customers without a maintenance contract should contact their local sales representative.

References

- https://www.openssl.org/news/secadv_20150319.txt

Legal disclaimer

WHILE EVERY REASONABLE EFFORT IS MADE TO PROCESS AND PROVIDE INFORMATION THAT IS ACCURATE, ALL THE CONTENT AND INFORMATION IN THIS DOCUMENT ARE PROVIDED "AS IS" AND “AS AVAILABLE,” WITHOUT ANY REPRESENTATION OR ENDORSEMENT AND WITHOUT ANY EXPRESS OR IMPLIED GUARANTEE OF CURRENCY, COMPLETENESS OR SUITABILITY, OR ANY WARRANTY INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE OR PURPOSE. YOUR USE OF THIS DOCUMENT, ANY INFORMATION PROVIDED, OR OF MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. VASCO RESERVES THE RIGHT TO CHANGE OR UPDATE THE INFORMATION IN THIS DOCUMENT AT ANY TIME AND AT ITS DISCRETION, AS AND WHEN NEW OR ADDITIONAL INFORMATION BECOMES AVAILABLE.