VASCO Security Advisory

Multiple OpenSSL Vulnerabilities Affecting VASCO products

Advisory ID: vasco-sa-20140605-openssl

Revision number: 1.0

Date and time of release: June 19 2014 15:00 UTC

Date and time of last update: June 19 2014 15:00 UTC

Summary

On June 5 2014 the OpenSSL Project published a security advisory describing seven vulnerabilities in the OpenSSL library. The vulnerabilities are referred to as follows:

- SSL/TLS MITM vulnerability
- DTLS Recursion flaw
- DTLS Invalid Fragment vulnerability
- SSL_MODE_RELEASE_BUFFERS NULL pointer dereference
- SSL_MODE_RELEASE_BUFFERS session injection or denial of service
- Anonymous ECDH denial of service
- ECDSA NONCE Side-Channel recovery attack

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

Following products are affected by the SSL/TLS MITM vulnerability:

SSL/TLS servers

- IDENTIKEY Server 3.3, 3.4
- IDENTIKEY Authentication Server 3.4 SR1, 3.5
- IDENTIKEY Federation Server 1.3, 1.4, 1.5
- IDENTIKEY (Virtual) Appliance 3.4.5.{0,1}
- IDENTIKEY (Virtual) Appliance 3.4.6.{0,1,2,3}
- IDENTIKEY (Virtual) Appliance 3.5.7.{1,2,3,4}
- aXsGUARD Gatekeeper 7.0.0 PL19, 7.1.0 PL6, 7.6.5, 7.7.0, 7.7.1, 7.7.2

SSL/TLS clients

- LDAP Synchronization Tool 1.1, 1.2
- Data Migration Tool 2.0, 2.1, 2.2, 2.3, 2.4
- DIGIPASS Authentication for Windows Logon 1.1, 1.2
- DIGIPASS Authentication for Citrix Web Interface 3.3, 3.4, 3.5, 3.6
- DIGIPASS Authentication for IIS - Basic 3.3, 3.4, 3.5
- DIGIPASS Authentication for Outlook Web Access - Basic 3.3, 3.4, 3.5
- DIGIPASS Authentication for Outlook Web Access - Forms 3.3, 3.4, 3.5
- DIGIPASS Authentication for Remote Desktop Web Access 3.4, 3.5, 3.6
- DIGIPASS Authentication for Steel-Belted RADIUS Server 3.2, 3.3
- Personal aXsGUARD 1.1.3, 2.1.0

Following products are affected by the SSL_MODE_RELEASE_BUFFERS NULL pointer dereference vulnerability:

- IDENTIKEY Federation Server 1.3, 1.4, 1.5
- aXsGUARD Gatekeeper 7.7.0, 7.7.1, 7.7.2

Following products are affected by the SSL_MODE_RELEASE_BUFFERS session injection or denial of service vulnerability:

- IDENTIKEY Federation Server 1.3, 1.4, 1.5
- aXsGUARD Gatekeeper 7.7.0, 7.7.1, 7.7.2

Detailed description of vulnerability

On June 5 2014 the OpenSSL Project published a security advisory describing seven vulnerabilities in the OpenSSL library.

The impact of this vulnerability on VASCO products varies depending on the affected product.

SSL/TLS Man-in-the-Middle

An unauthenticated, remote attacker with the ability to intercept traffic between an affected SSL/TLS client and SSL/TLS server could execute a man-in-the-middle attack. This vulnerability has been assigned CVE-2014-0224.

SSL_MODE_RELEASE_BUFFERS NULL pointer dereference

An unauthenticated, remote attacker could submit a malicious request designed to trigger a NULL pointer dereference. This could result in a partial or complete denial of service condition on the affected device. This vulnerability has been assigned CVE-2014-0198.

SSL_MODE_RELEASE_BUFFERS session injection or denial of service

An unauthenticated, remote attacker could submit a malicious request designed to inject content into a parallel SSL/TLS session or create a denial of service condition. This vulnerability has been assigned CVE-2010-5298.

For additional details, customers are referred to the OpenSSL Project security advisory: http://www.openssl.org/news/secadv_20140605.txt

Severity score

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

SSL/TLS Man-in-the-Middle

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

CVSS Temporal Score: 3.6		
Exploitability	**Remediation Level**	**Report Confidence**

Functional	Official Fix	Confirmed

SSL_MODE_RELEASE_BUFFERS NULL pointer dereference

CVSS Base Score: 7.1					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None	None	None	Complete

CVSS Temporal Score: 7.8		
Exploitability	**Remediation Level**	**Report Confidence**
Functional	Official Fix	Confirmed

SSL_MODE_RELEASE_BUFFERS session injection or denial of service

CVSS Base Score: 7.8					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None	None	Partial	Complete

CVSS Temporal Score: 6.4		
Exploitability	**Remediation Level**	**Report Confidence**
Functional	Official Fix	Confirmed

Product fixes and workarounds

VASCO has released patches for following products:

- IDENTIKEY Federation Server 1.3.2, 1.4.2, 1.5.1 on June 13 2014

VASCO will release following patches:

- IDENTIKEY Authentication Server 3.5.4 on June 23 2014
- IDENTIKEY (Virtual) Appliance 3.5.7.5 on June 23 2014
- aXsGUARD Gatekeeper 7.7.3, the release date of which will be announced later

Customers using IDENTIKEY Server 3.3 or 3.4 and customers using IDENTIKEY Authentication Server 3.4 SR1 are recommended to upgrade to IDENTIKEY Authentication Server 3.5 and apply the appropriate fix for this version.

Customers using aXsGUARD Gatekeeper are recommended to upgrade to aXsGUARD Gatekeeper 7.7.3.

Customers using a client-side product affected by the SSL/TLS Man-in-the-Middle vulnerability are recommended to upgrade the corresponding server-side product. This approach will avoid any impact as both a vulnerable client-side and server-side product are required to exploit the vulnerability.

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from MyMaintenance.

References

- http://www.openssl.org/news/secadv_20140605.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.