VASCO Security Advisory

OpenSSL Heartbleed Vulnerability in VASCO products

Advisory ID: vasco-sa-20140417-heartbleed

Revision number: 1.3

Date and time of release: April 17 2014 13:20 UTC

Date and time of last update: May 12 2014 15:00 UTC

Summary

Multiple VASCO products incorporate a version of the OpenSSL library affected by a vulnerability that could allow an unauthenticated, remote adversary to retrieve portions of 64 kilobytes from the memory of the VASCO client or server product. This vulnerability is referred to as the Heartbleed bug.

The vulnerability is due to a missing bounds check in the handling of the Transport Layer Security (TLS) heartbeat extension, as specified in RFC 6520. An adversary could exploit this vulnerability by implementing a malicious TLS client, if trying to exploit the vulnerability on an affected server, or a malicious TLS server, if trying to exploit the vulnerability on an affected client. An exploit could send a specially crafted heartbeat packet to the connected client or server. An exploit could allow the adversary to disclose 64 kilobytes of memory from a connected client or server for every heartbeat packet sent. The disclosed portions of memory could include sensitive information such as private keys and application-specific data.

This vulnerability is referred to using the Common Vulnerabilities and Exposures ID CVE-2014-0160.

Impacted products

The following VASCO products are affected by the Heartbleed bug:

- Personal aXsGUARD 2.0.0
- IDENTIKEY Authentication server and Patch 3.5.1
- IDENTIKEY Appliance 3.5.7.0, 3.5.7.1 and 3.5.7.2
- IDENTIKEY Virtual Appliance 3.5.7.0, 3.5.7.1 and 3.5.7.2
- IDENTIKEY Federation Server 1.3 and 1.4
- MYDIGIPASS.COM
- DIGIPASS Authentication for Windows Logon 1.2.0
- LDAP Synchronization Tool 1.3.0
- DIGIPASS Authentication for IIS 3.5.0, DIGIPASS Authentication for Citrix Web Interface V3.6.0, DIGIPASS Authentication for Outlook Web Access 3.5.0, DIGIPASS Authentication for Remote desktop Web Access 3.5.0, DIGIPASS Authentication for SBR 3.5.

The aXsGUARD GateKeeper appliances and other VASCO products are not affected by this bug.

Detailed description of vulnerability

The impact of this vulnerability on VASCO products varies depending on the affected product. Successful exploitation of the vulnerability may cause portions of memory from a client or server to be disclosed. The disclosed portions of memory could include sensitive information such as private keys and application-specific data.

Severity score

The table below denotes the CVSS 2.0 vulnerability score.

CVSS Base Score: 5					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Low	None	Partial	None	None

CVSS Temporal Score: 5		
Exploitability	**Remediation Level**	**Report Confidence**
High	Unavailable	Confirmed

Product fixes and workarounds

VASCO has updated its MYDIGIPASS.COM authentication service on April 9 2014.

VASCO has released patches for following products:

- IDENTIKEY Federation Server 1.4.1, released on April 10th 2014
- IDENTIKEY Federation Server 1.3.1, released on April 11th 2014
- IDENTIKEY Authentication server 3.5.2, released on April 18th 2014
- IDENTIKEY Appliance 3.5.7.3, released on April 18th 2014
- IDENTIKEY Virtual Appliance 3.5.7.3, released on April 18th 2014
- DIGIPASS Authentication for Windows Logon V1.2.1, released on April 30th 2014
- LDAP Synchronization Tool V1.3.2, released on May 9th 2014.
- DIGIPASS Authentication for Citrix Web Interface V3.6.1, released on May 9th 2014.
- DIGIPASS Authentication for OWA Basic 3.5.1, released on May 9th 2014.
- DIGIPASS Authentication for OWA Forms 3.5.1, released on May 9th 2014.
- DIGIPASS Authentication for IIS Basic 3.5.1, released on May 9th 2014.
- DIGIPASS Authentication for Remote Desktop Web Access 3.6.1, released on May 9th 2014.
- DIGIPASS Authentication for Steel-Belted RADIUS Server 3.3.1, released on May 9th 2014.

VASCO will release following patches:

- Personal aXsGUARD 2.1.0

Customers with affected products should take following three steps to mitigate the vulnerability:

A. **Step 1: upgrade all affected products using the fixed product releases provided by VASCO**

B. **Step 2: revoke SSL/TLS private keys and issue new key pairs and certificates.** Due to the bug, it cannot be excluded that SSL/TLS private keys are compromised. Therefore customers should revoke their existing key pairs and certificates and issue new ones.

C. **Step 3: update sensitive data exchanged using SSL/TLS.** Customers should assess whether sensitive data (e.g. user passwords, credit card details) exchanged over SSL/TLS might have been compromised. This assessment is specific to the customer. If sensitive data is affected, customers should consider updating this data as well.

Obtaining product releases with fixes

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

References

- http://heartbleed.com
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
- Heartbleed Two-Factor Authentication Emergency Room
- Addressing the Heartbleed OpenSSL Bug in Financial Institutions
- Addressing the Heartbleed OpenSSL Bug on MYDIGIPASS.COM
- Increasing resilience against Heartbleed-alike bugs using Two-Factor Authentication

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.