

## Reflected cross-site scripting vulnerability in IDENTIKEY Authentication Server help function

Advisory ID: vasco-sa-20150903-ias

Revision number: 1.0

Date and time of release: September 03 2015 12:00 UTC

Date and time of last update: September 03 2015 12:00 UTC

### Summary

Information security auditors from the company Security B.V. have privately reported a cross-site scripting vulnerability that is present in the help function of IDENTIKEY Authentication Server and IDENTIKEY (Virtual) Appliance installations.

### Impacted products

- IDENTIKEY (Virtual) Appliance versions 3.8 and earlier
- IDENTIKEY Authentication Server versions 3.8 and earlier

### Detailed description of vulnerability

The web administration section of IDENTIKEY Authentication Server and IDENTIKEY (Virtual) Appliance also contains a help function. The help function is accessible in a subdirectory of the web administration section. A cross-site scripting vulnerability has been found in this help function.

In order to open the help on a particular page, a special parameter can be passed as part of the help section URL. When replacing the value of this parameter with a specially crafted cross-site scripting attack vector, the attack vector will be executed in the context of the end-user's browser.

### Severity score

The table below denotes the CVSS 2.0 vulnerability score of the vulnerability.

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

### Product fixes and workarounds

VASCO will fix these vulnerabilities in the following upcoming releases

- IDENTIKEY (Virtual) Appliance 3.9
- IDENTIKEY Authentication Server 3.9

## **Obtaining product releases with fixes**

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

## **Acknowledgements**

VASCO recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure. See our [Hall of Fame](#) for more information.

## **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.

Copyright © 2015 VASCO Data Security, Inc., VASCO Data Security International GmbH. All rights reserved.