VASCO Security Advisory

Open redirect and cross-site scripting vulnerabilities in VASCO IDENTIKEY products

Advisory ID: vasco-sa-20141029-xss

Revision number: 1.1

Date and time of release: October 29 2014 12:00 UTC+1

Date and time of last update: November 13 2014 12:00 UTC+1

Summary

On September 23 2014 VASCO became aware of an open redirect and cross-site scripting vulnerabilities in VASCO IDENTIKEY Authentication Server Websites and IDENTIKEY Appliance Administration Website. The open redirect vulnerability could be used in phishing attacks to get users to visit malicious sites without realizing it, while the cross-site scripting vulnerabilities could allow an attacker to inject malicious scripts into web pages, and gain elevated access-privileges to sensitive page content, session cookies, and other information.

Impacted products

Following products are affected by the vulnerabilities:

- IDENTIKEY Authentication Server 3.3 to 3.6.
- IDENTIKEY Authentication Server Websites part of IDENTIKEY Appliance 3.4.6.2 to 3.6.8.0.
- IDENTIKEY Appliance 3.5.7.{1-6} and 3.6.8.0.

Detailed description of the vulnerabilities

The VASCO IDENTIKEY Authentication Server Websites are subject to an open redirect vulnerability that could allow an attacker to perform phishing attacks. They also are subject to cross-site scripting vulnerabilities that could allow an attacker to inject malicious scripts into the affected web pages, and use this attack vector to e.g. steal session cookies.

The VASCO IDENTIKEY Appliance Administration Website is subject to a cross-site scripting vulnerability that could allow an attacker to inject malicious scripts into the affected web page, and use this attack vector to e.g. steal session cookies.

Severity score

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

<table>
<tr><td colspan="6"><b>CVSS Base Score:</b> 5.0</td></tr>
<tr><td><b>Access Vector</b></td><td><b>Access Complexity</b></td><td><b>Authentication</b></td><td><b>Confidentiality Impact</b></td><td><b>Integrity Impact</b></td><td><b>Availability Impact</b></td></tr>
<tr><td>Network</td><td>Low</td><td>None</td><td>Partial</td><td>None</td><td>None</td></tr>
<tr><td colspan="6"><b>CVSS Temporal Score:</b> 4.8</td></tr>
<tr><td colspan="2"><b>Exploitability</b></td><td colspan="2"><b>Remediation Level</b></td><td colspan="2"><b>Report Confidence</b></td></tr>
<tr><td colspan="2">Functional</td><td colspan="2">Unavailable</td><td colspan="2">Confirmed</td></tr>
</table>

Product fixes and workarounds

VASCO will release following patches:

- IDENTIKEY Authentication Server Websites 3.6.1, on November 28, 2014
- IDENTIKEY Appliance 3.6.8.1, on November 28 2014

Customers who have deployed one of the impacted IDENTIKEY Authentication Server Websites standalone packages must uninstall this package and install IDENTIKEY Authentication Server Websites 3.6.1.

Customers who have deployed the impacted IDENTIKEY Authentication Server Websites as part of the IDENTIKEY Authentication Server must uninstall this feature from their IDENTIKEY Authentication Server installation and install IDENTIKEY Authentication Server Websites 3.6.1.

Customers using impacted versions of IDENTIKEY Appliance are recommended to upgrade to IDENTIKEY Appliance 3.6.8.1.

Obtaining product releases with fixes

- For IDENTIKEY Authentication Server:

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

- For IDENTIKEY Appliance:

  Customers with a maintenance contract can obtain fixed product releases from MyMaintenance or choose for online update in IDENTIKEY Appliance's update wizard. Customers without a maintenance contract should contact their local sales representative.

References

VASCO would like to thank Richard Dalton from Rits Information Security for reporting the vulnerabilities to VASCO PSIRT.

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.