VASCO Security Advisory

Reflected cross-site scripting vulnerability in DIGIPASS authentication for Citrix Web Interface

Advisory ID: vasco-sa-20150903-DPAuth4CWI

Revision number: 1.0

Date and time of release: September 3 2015 12:00 UTC

Date and time of last update: September 3 2015 12:00 UTC

Summary

Information security auditors from the company Integrity have privately reported a cross-site scripting vulnerability that may be present in Citrix Web Interface installations that use VASCO's *DIGIPASS authentication for Citrix Web Interface* plugin. The issue is present in the login page of the Citrix Web Interface.

Impacted products

Following products are affected by vulnerability:

- DIGIPASS authentication for Citrix Web Interface

Detailed description of vulnerability

The DIGIPASS Authentication Plug-In may be configured to pass information to Citrix when it fails an authentication request. This information may be used to provide users with an explanation of why their login failed, and steps that they may be able to take to rectify the problem. The DIGIPASS Authentication Plug-In will pass the error or status code and message text for the authentication server to Citrix, which may then display the message verbatim or interpret the code to provide the user with a clear explanation or set of instructions.

As part of the installation package VASCO provides a sample feedback.inc file that customers should copy into the Citrix installation directory. The code in the feedback.inc file is executed during the loading of the Citrix Web interface login page. The sample code displays error or status code and the message text without applying input filtering, which results in a reflected cross-site scripting vulnerability.

Customers are only vulnerable if they have replaced the feedback.inc file with the sample file provided by VASCO, or if they have updated their feedback.inc file using the sample code available in the product documentation.

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

Since the approaching end-of-maintenance date set by Citrix for its Citrix Web Interface product, VASCO will not release an update of the DIGIPASS Authentication Plug-In for Citrix Web Interface. Instead customers who have modified the feedback.inc file of their Citrix Web Interface product should apply the workaround documented below.

In order to remediate this issue, an impacted customer may use one of following solutions:

1) The customer may replace the feedback.inc file with the original feedback.inc file that was provided by Citrix. In this case the customer must set the flag 'Return failure reason' unchecked in the DIGIPASS Authentication Plug-In Configuration Center.
2) The customer may edit the feedback.inc file and remove or comment out the code that displays the DIGIPASS failure reason. Customers should follow this approach if the original feedback.inc file is no longer available.

More details about these solutions are available in VASCO's Knowledge Base article KB 140148.

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.