Mini Bulletin XRX19Z

Xerox® DocuShare® 6.5.3 through 7.0.0
SPAR Release ds653to700cleanuptoolp1

Bulletin Date: October 1, 2019

Purpose

This Bulletin is intended ONLY for the specific security problems identified below. The problem identified has been rated a criticality level of IMPORTANT.

Includes fix for the following vulnerability:

- A Reflected Cross-Site Scripting (XSS) vulnerability in the webEx module in webExMeetingLogin.jsp and deleteWebExMeetingCheck.jsp in Fuji Xerox DocuShare through 7.0.0.C1.609 allows remote attackers to inject arbitrary web script or HTML via the handle parameter (webExMeetingLogin.jsp) and meetingKey parameter (deleteWebExMeetingCheck.jsp) (CVE-2019-16307).

- The Xerox products affected are DocuShare server versions 6.5.3 through 7.0, running on Windows, Solaris and Linux operating systems.

Acknowledgments

Xerox wishes to thank Witsarut Limsuwan for initially notifying us of the Reflected Cross-Site Scripting (XSS) vulnerability.

Software Release Details

If your software is higher or equal to the versions listed below no action is needed.

Otherwise, please review this bulletin and consider installation of this version.

Software	DocuShare
System SW version	ds653to700cleanuptoolp1
Link to SW update & Install Inst	Available here[1]

Unzip the file to a known location on your workstation/computer.

[1] For questions or further support on this patch please e-mail docushare.support@xerox.com or call 1-800-835-9013

xerox™