

# Mini Bulletin XRX20W

Xerox® DocuShare

Release 6.61, 7.0, and 7.5

Bulletin Date: November 30, 2020

## Purpose

This Bulletin is intended ONLY for the specific security issue identified below which has been rated with a criticality level of IMPORTANT.

This is a hotfix that includes fixes for the following vulnerabilities:

- CVE-2020-27177 - Unauthenticated external XML entity injection
- Server-Side Request Forgery

## Software Release Details

Please review this bulletin and consider installing the hotfix for your configuration.

DocuShare 7.5 - DocuShare 7.5 Hotfix 2

DocuShare 7.0 - DocuShare 7.0.0 Update 1 Patch 3 Hotfix 22

DocuShare 6.6.1 - DocuShare 661 Update 3 Patch 4 Hotfix 9

Configuration	DocuShare 6.6.1	DocuShare 7.0	DocuShare 7.5
Solaris	<a href="#">Available here</a>	<a href="#">Available here</a>	N/A
Windows	<a href="#">Available here</a>	<a href="#">Available here</a>	<a href="#">Available here</a>
Linux	<a href="#">Available here</a>	<a href="#">Available here</a>	<a href="#">Available here</a>

## Acknowledgement

Xerox would like to thank Julien Ahrens for informing us of the need to address the security issue.

