# Security Bulletin XRX19-027

## Xerox® Docushare®

# Address Remote Method Invocation (RMI) Remote Execution Vulnerability

Bulletin Date: October 23, 2019

## Background

A Remote Method Invocation (RMI) remote execution vulnerability exists that could allow remote attackers to call executables on a server hosting DocuShare. This attack can occur if the RMI remote access port is bound to an external network adapter and not blocked by a firewall rule.

RMI is a Java API that supports direct transfer of serialized Java classes in a distributed network. DocuShare requires RMI to be enabled for internal communications. By default, the RMI service is exposed externally on port 1099/TCP to provide open interoperability with RMI clients. If this port is exposed to untrusted endpoints without additional security controls the system may be at risk.

Mitigation of this vulnerability relies on the proper safeguards of the network environment in which DocuShare operates. These proper safeguards should include the following:

- The RMI port (1099 by default) should never be open to the Internet. This port should be blocked to the internet via the company firewall.
- The RMI port (1099 by default) should not be open outside of the host machine. Preferably, the port should not be bound to an external network interface (only local loopback); alternatively, it may be blocked via a local firewall on the server DocuShare is installed on.
- If the RMI port needs to be open for intranet, security controls should be employed to prevent unauthorized access (such as use segmentation, firewall, host access controls, etc.).
- Change the RMI port to another one that is not the default 1099 port.
- Apply the latest DocuShare updates and patches from https://www.support.xerox.com/support/xerox-docushare/software/. Xerox recommends customers running older versions of DocuShare upgrade their system to DocuShare 7.0 for better security.
- Deploy anti-virus software that can detect RMI attacks on the server.
- For better security the documents stored in DocuShare should be encrypted using the DocuShare Content Encryption add-on.
- Follow industry or company best practices to secure access to the servers DocuShare and its components run on.

### Applicability

This vulnerability affects all versions of DocuShare. However, DocuShare Flex is not impacted by this vulnerability.

### Acknowledgement

Xerox would like to thank Brenden Meeder for informing us of this vulnerability.