Security Patch Criticality Rating

September 2020

Document Version: 1.0 (September 2020).

Contents

1. Introduction 1

2. Security Patch Criticality Overview...1

Security Patch Rating Scope 1

Security Patch Criticality Ratings Definitions 2

Considerations Before Patching 2

Table 1: Security Problem Severity Category Definitions 3

Security Patch Ratings..4

Table 2: Security Patch Criticality Categories and Recommended Install Actions 4

1. Introduction

Since 2004 Xerox has been providing security patches to our customers to address vulnerabilities found both internally and externally in Xerox® Products. Xerox has been doing this to provide customers with the assurance that Xerox takes the security of the software and firmware included in Xerox® Products very seriously, and that we will proactively address security problems in our products as we become aware of them.

We are continuously working to improve the internal processes used to implement and test security patches in a timely manner. We also only post security patches on our Security Website that are considered crucial to our customers:

http://www.xerox.com/information-security/xerox-security-bulletins/enus.html

For each of the security patches posted, we recommend that patches be installed on the applicable products as soon as possible. Customers may, however, need explicit recommendations for posted security patches so they can adequately plan when and how quickly they need to apply security patches. The purpose of this document is to describe our Security Patch Rating System which provides guidance customers may find helpful.

This document does not address any issues associated with charges for installation of security patches on customer machines.

2. Security Patch Criticality Overview

Security Patch Rating Scope

This document covers security patches that are posted on the Xerox Security Web Site www.xerox.com/security for any Xerox® Products that are currently being marketed or maintained. In addition, patches will only be created for the products and releases affected by the security problem(s) being resolved.

Security Patch Criticality Ratings Definitions

The Xerox Security Patch Ratings are determined by weighting the following factors:

1. Severity rating for the security problem(s) being resolved by the security patch. The security problem severity categories range from ‘Critical’ down to ‘Low’. The Xerox security problem severity definitions used here are defined in **Table 1** on page 3 of this document.
2. A determination as to whether, for the indicated security problem:
   - An exploit exists.
   - The exploit has been implemented external to Xerox.
   - The exploit has been made known to Xerox.
   - The exploit has been made known publicly.
3. A determination of the scope of the problem in terms of how many Xerox® Product families and system software releases are or could be affected by the problem and the resultant fix.
4. Whether the problem once exploited could expose customer networks, customer image data or both.

Considerations Before Patching

The Installation Instructions contained in each security bulletin will clearly indicate the affected products as well as the system software/network controller release which the security patch should be installed on. Please read all Security Bulletins and accompanying Installation Instructions carefully to understand the requirements for upgrade and determination of affected software levels that will require a patch.

TABLE 1: SECURITY PROBLEM SEVERITY CATEGORY DEFINITIONS

Severity	Definition
Critical	A vulnerability whose exploitation could allow an attacker to take over the system and execute arbitrary code.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user's data, or of the integrity or availability of processing resources.
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

Security Patch Install Responsibility

It should be noted that not all patches are "customer installable". Where the Security Bulletin states that a patch can be downloaded and installed by the customer, application of the patch is the customer responsibility1. When a Security Bulletins states that a patch is not customer installable, it is then the responsibility of Xerox to apply the patch.

For some products (e.g., products that use a Xerox® FreeFlow® Print Server Digital Front End) a Xerox Customer Service Engineer is required to install any security patch. Refer to the applicable Security Bulletin in each case for specific details.

Customers should determine the best approach for installing patches based on their ability to install, the patch criticality rating and/or applicability to the customer environment. This would include either contacting Xerox to install the patch (not customer installable), self-installation at the earliest opportunity based on customer polices/environment (customer installable) or waiting until the next scheduled service call to have a patch applied.

[1] Security Patches and/or upgrades that are considered "Customer Installable" are the responsibility of the Customer and as such are not covered by the Maintenance Agreement unless explicitly called out in the Managed Services Contract.

Security Patch Ratings

Based on an assessment of the four sets of factors above in Table 1, the security patch is given one of the Security Patch Criticality Ratings shown in Table 2 below. It should be noted that along with the Security Patch Criticality Rating, Table 2 also indicates the recommended customer installation action for the security patch.

TABLE 2: SECURITY PATCH CRITICALITY CATEGORIES AND RECOMMENDED INSTALL ACTIONS

			Installation Action Based on Install Responsibility	
Patch Rating	**Security Problems Addressed**	**Key Exploit Factors**	**Customer Installable:** Patch Can Be Applied by Customer per the Security Bulletin (Customer Responsibility)	**Not Customer Installable:** Patch Cannot Be Applied by Customer per Security Bulletin (Xerox Responsibility)
Critical	Patch resolves at least one (1) security problem with critical severity	Exploit is publicized external to Xerox **and** Exposes customer networks, image data or PII/CII[2]	Install patch as soon as possible.	Contact Xerox customer support ASAP to arrange patch installation if applicable to the customer environment
Important	Patch resolves zero (0) security problems with Critical severity and at least one (1) security problem with Important severity	Xerox recognized exploit exists	Install patch at the earliest opportunity per customer policies or if applicable to customer environment	Have Xerox Service install patch at next scheduled service call if applicable to the customer environment
Moderate	Patch resolves zero (0) security problems with either Critical or Important severity and at least one (1) security problem with Moderate severity	Xerox recognized exploit exists	Consider applying patch per customer policies or if applicable to customer environment	Consider having Xerox Service install patch at next scheduled service call if applicable to customer environment.

[2] Personal Identifiable Information/Customer Identifiable Information