Security Patch
Criticality Rating

May 22, 2017

Document Version: 2.4 (May 2017)

Contents

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 our 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.

Xerox has been working to improve the internal processes used to implement and test security patches in a timely manner. Xerox's view to date has been that only security patches that we consider critical to our customers are posted on the Security Web Site:

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

For each of the security patches posted, there is the implicit recommendation that the patches be installed on the applicable products as soon as possible. However, we have become aware that for many customers this implicit recommendation is not adequate enough – they would like for Xerox to provide a more explicit recommendation accompanying each security patch posted so they can adequately plan when and how quickly they need to install each patch.

In response to this request Xerox developed a Security Patch Rating system in late 2007 to provide the desired explicit recommendations to customers for each posted security patch. Xerox revised the ratings in late 2009. The purpose of this document is to describe this Security Patch Rating system.

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

Security Patch Ratings 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.

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 below.
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.

Table 1 Security Problem Severity Category Definitions

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.

Table 2 Security Patch Criticality Categories

Note: 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.

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

Patch Rating	Security Problems Addressed	Key Exploit Factors	Installation Action	
			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[1]	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	Exploit exists and is known to Xerox	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	Exploit exists and is known to Xerox	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.

[1] Personal Identifiable Information/Customer Identifiable Information

Table 2 Notes

1. The indicated customer installation actions are recommendations only. It is up to the individual customer to determine based on that customer's security or IT policies how quickly and to what extent each software patch will be installed.
2. Some security patches may require a software upgrade before the patch can be successfully installed. If that is the case, this fact will be clearly indicated in the Installation Instructions accompanying the applicable Security Bulletin. In the case of a Critical software patch the Installation Instructions will clearly indicate if any required software upgrade will be mandatory. This assessment will be based on analysis of the associated exploit(s) and the factors described in the Security Patch Criticality Ratings Definitions section of this document.
3. Security patches will only be created for the products and releases affected by the security problem(s) being resolved. The Installation Instructions contained in each security bulletin will clearly indicate what products are affected by the software patch and which specific product system software/network controller releases for the affected products the security patch should be installed on. Please read the Security Bulletins and accompanying Installation Instructions carefully, because for some affected products certain system software releases may not require that the software patch be installed.
4. 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.