Vulnerability Management and Disclosure Policy

Version 5.0

October 3, 2015

Document Version: 5.0 (August 2015).

Table of Contents

1. Introduction 3
2. Security Built In 3
3. Where We Look 4
4. How We Work 4

Introduction

As a leader in the development of digital imaging technology, Xerox Corporation has demonstrated a commitment to keeping digital devices and information secure by proactively identifying potential vulnerabilities in our products. Additionally, Xerox practices responsible disclosure when, in the course of our development and testing, we discover a vulnerability in products obtained from our vendors. We cooperate with the vendor to support them in fixing vulnerabilities and improving the security of their products.

Security Built In

Our commitment to Xerox product security begins early in product development with secure coding techniques, extensive testing, and analysis to eliminate vulnerabilities. Xerox actively engages certification practices such as Common Criteria and is active in emerging standards such as P2600 Working Group and the Software Development Lifecycle.

There are cases where new vulnerabilities occur after products are in the field. It is Xerox policy to repair these vulnerabilities in as timely a manner as possible and practice responsible disclosure to our customers. Factors such as complexity of the system and severity of the vulnerability can cause this reaction time to vary between products and offerings.

Security Information for Xerox products and services is available at:

www.xerox.com/security

Where We Look

The following table contains the primary sources that are monitored by Xerox Corporation to discover vulnerabilities.

We review each new notification from these sources, evaluate and rank each vulnerability to determine the applicability to Xerox products. We monitor for vulnerabilities in technologies developed by Xerox, and in products purchased from partner vendors. If vulnerabilities affect Xerox products, we work to incorporate a patch as soon as practical.

Source	Description
US-CERT www.us-cert.gov	United States Computer Emergency Response Team Detailed list of vulnerabilities of many operating systems and software applications. Published in e-mail form weekly.
Oracle Critical Patch Update (CPU) Report http://www.oracle.com/technetwork/topics/security/securityemail-090378.html Follow instructions to create an account.	A comprehensive list of vulnerabilities of the Solaris Operating System and associated applications. Published in e-mail form quarterly.
Secunia www.secunia.com	Web site with a comprehensive list of security vulnerabilities.
BugTraq www.securityfocus.com	Mailing List dedicated to security vulnerabilities.
Microsoft Security Bulletins **Microsoft Security** Response Center (MSRC)	Comprehensive list of vulnerabilities of the Microsoft Operating Systems and Applications. Published monthly via the Microsoft Bulletin process.

In addition to reviewing the industry standard sources, Xerox actively collaborates with industry security experts, who submit vulnerability identification data and support information through the Security@Xerox web site,

How We Work

Because the scope of the vulnerability can change widely, the timeframe for delivery of a solution can vary as well.

For Xerox to deliver a solution, we take a number of steps to ensure problems are fixed correctly the first time. We test and validate all fixes, and plan a proper delivery method for supplying the fix to our customers.

Depending on a number of factors, the fix for a given vulnerability may be delivered as a separate patch or in the next release of the affected systems software.