

## 1.0 Xerox Office Group Security Patch Criticality Ratings

Since 2004 Xerox has been providing security patches to our customers to address vulnerabilities found both internally and externally in Xerox Office Group (XOG) 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 our XOG products very seriously, and that we will proactively address security problems in our products as we become aware of them.

XOG has been working the past two years to improve the internal processes used to implement and test security patches in a timely manner. XOG's view to date has been that only security patches that we consider critical to our customers are posted on the Security Web Site [www.xerox.com/security](http://www.xerox.com/security), so 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 XOG 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 XOG has developed a Security Patch Rating system to provide the desired explicit recommendations to customers for each posted security patch. The purpose of this document is to describe this new Security Patch Rating system.

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

### 1.1 Security Patch Ratings Scope

This document covers security patches that are posted on the Xerox Security Web Site [www.xerox.com/security](http://www.xerox.com/security) for any XOG product that are currently being marketed or maintained.

### 1.2 Security Patch Criticality Ratings Definitions

The XOG 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 XOG security problem severity definitions used here are defined in Table 1.
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 XOG 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 compromise customer networks, customer data or both.

Based on an assessment of these four sets of factors, 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 whether a Security Bulletin accompanying the patch will be posted on the Xerox Security Web Site, and the recommended customer action for the security patch.

This Page is Intentionally Left Blank

**Table 1. Security Problem Severity Category Definitions**

<u>Severity</u>	<u>Severity Definition</u>
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**

<u>Patch Criticality Category</u>	<u>Security Problem(s) Addressed</u>	<u>Key Exploit Factors</u>	<u>Customer Installation Recommendation</u>		<u>Security Bulletin Issued</u>
			<u>Patch Can Be Applied By Customer</u>	<u>Patch Cannot Be Applied By Customer</u>	
Critical	Patch resolves at least one (1) security problem with Critical severity	<ul style="list-style-type: none"> <li>Exploit exists and is known to Xerox</li> <li>Exploit external to Xerox or exploit publicized</li> <li>Compromises customer networks or data</li> </ul>	Install Patch as soon as possible	Contact Xerox Customer Support ASAP to Arrange Patch Installation	<b>Yes</b>
Important	Patch resolves zero (0) security problems with Critical severity and at least one (1) security problem with Important severity	<ul style="list-style-type: none"> <li>Exploit exists and is known to Xerox</li> <li>Compromises customer networks or data</li> </ul>	Install Patch as soon as Possible	Have Xerox Service Install Patch at Next Scheduled Service Call	<b>Yes</b>
Moderate	Patch resolves zero (0) security problems with either Critical or Important severity and at least one (1) security problem with	<ul style="list-style-type: none"> <li>Exploit exists and is known to Xerox</li> </ul>	Install Patch Per Customer Policies or if Applicable to Customer Environment	Have Xerox Service Install Patch at Next Scheduled Service Call if Applicable to Customer Environment	<b>Yes</b>

<u>Patch Criticality Category</u>	<u>Security Problem(s) Addressed</u>	<u>Key Exploit Factors</u>	<u>Customer Installation Recommendation</u>		<u>Security Bulletin Issued</u>
			<u>Patch Can Be Applied By Customer</u>	<u>Patch Cannot Be Applied By Customer</u>	
	Moderate severity				

**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 Section 1.2.
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.

**Disclaimer**

The information provided in this document is provided "as is" without warranty of any kind. Xerox Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including, without limitation, direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

XEROX®, The Document Company®, the digital X®, and all Xerox product names are trademarks of XEROX CORPORATION. Other trademarks belong to their respective owners.

Copyright © XEROX CORPORATION 2007. All Rights Reserved