

Use of CA-signed Digital Certificates for Better Security

v1.0
03/16/09

Background

A Signature Collision vulnerability¹ has been found in the use of the MD5 algorithm in applications like digital certificates. An attacker could take advantage of this vulnerability to create forged valid X.509 certificates for the purpose of conducting phishing attacks or for impersonating a legitimate site. This vulnerability has been noted in some Xerox WorkCentre Multi-function devices that use MD5 to create self-signed digital certificates.

As a workaround to this vulnerability, Xerox strongly recommends that when setting up a Machine Digital Certificate on the device to enable the use of Secure Sockets Layer (SSL) encryption, the customer should always use the "Certificate Signing Request" option which results in obtaining a digital certificate from a trusted Certificate Authority. In lieu of that the customer should use a digital certificate from a Third Party that is known to use either the SHA-1 or SHA-2 algorithm for creating the digital certificate. The customer should not use the 'Self Signed Certificate' option.

This workaround applies to the following Xerox WorkCentre/WorkCentre Pro products:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
5632	
5638	
5645	
5655	
5665	
5675	
5687	
7655	
7665	
7675	

Disclaimer

The information provided in this Xerox 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 Xerox Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

¹ For more details on this vulnerability see the information in URL <http://www.kb.cert.org/vuls/id/836068>.