Xerox Product Security

OpenSSL Vulnerabilities

Poodle, Freak and Logjam

Version 1.4
June 30, 2016

Disclaimer

The information provided in this Xerox® Product Response 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 held responsible 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 damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.

Summary Information

Three vulnerabilities in the OpenSSL libraries for SSL/TLS have been reported. These may open possibilities for man in the middle or brute force attempts to intercept data transmission possible. These vulnerabilities are commonly associated with the names Poodle, Freak and Logjam. Following is current status of many Xerox products.

Information is accurate for the latest device software available to customers. Xerox recommends customers update to the latest available release.

Xerox publishes security Mini Bulletins when vulnerabilities are remediated in product updates. Detailed security information can be found at (http://www.xerox.com/information-security/enus.html).

If additional information is needed, please contact Xerox technical support or submit a question here http://www.xerox.com/perl-bin/formeng.pl?form=product_security_information_request_7285 .

Poodle

Common vulnerability CVE-2014-3566. The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain clear text data via a padding-oracle attack, aka the "POODLE" issue.

Xerox has removed SSLv3 support or provided a means for customers to disable it. This mitigates the vulnerability. Status below is valid for the latest software version available to customers.

Monochrome Models		Vulnerable
Phaser®	3020	No
Phaser®	3052/3260	No
Phaser®	3300	No
Phaser®	3320	No
Phaser®	3600	No
Phaser®	3610	No
Phaser®	3635 MFP	No
Phaser®	4600/4620	No
Phaser®	4622	No
Phaser®	5550	No

Monochrome Models		Vulnerable
WorkCentre®	3025BI	No
WorkCentre®	3025NI	No
WorkCentre®	3210/3220	No
WorkCentre®	3215/3225	No
WorkCentre®	3315	No
WorkCentre®	3325	No
WorkCentre®	3550	No
WorkCentre®	3615	No
WorkCentre®	3655	No
WorkCentre®	4250	No
WorkCentre®	4260	No
WorkCentre®	4265	No
WorkCentre®	5135/5150	No
WorkCentre®	5225/5230	Yes
WorkCentre®	5325/5330/5335	No
WorkCentre®	5632/5638/5645/5655/5665/5675/5687	No
WorkCentre®	5735/5740/5745/5755/5765/5775/5790	No
WorkCentre®	5845/5855/5865/5875/5890	No
WorkCentre®	5945/5955	No

Poodle

Monochrome Models		Vulnerable
Xerox D Series	D95A/D110/D125	No
Xerox D Series	D136	No

Color Models		Vulnerable
ColorQube®	8570/8870	No
ColorQube®	8580/8880	No
ColorQube®	8700/8900	No
ColorQube®	9201/9202/9203 CBC	No
ColorQube®	9201/9202/9203 SBC	No
ColorQube®	9301/9302/9303	No

Color Models		Vulnerable
Phaser®	6000/6010	Yes
Phaser®	6020 Windows	No
Phaser®	6020 Mac	No
Phaser®	6022 Windows	No
Phaser®	6022 Mac	No
Phaser®	6128/6128MFP	Yes
Phaser®	6280	No
Phaser®	6500	No
Phaser®	6600	No
Phaser®	6700	No
Phaser®	7100	Yes
Phaser®	7500	No
Phaser®	7800	No

Color Models		Vulnerable
WorkCentre®	6015 N/NI	Yes
WorkCentre®	6025 Windows	No
WorkCentre®	6025 Mac	No
WorkCentre®	6027 Windows	No
WorkCentre®	6027 Mac	No
WorkCentre®	6400	No
WorkCentre®	6505	No
WorkCentre®	6605	No
WorkCentre®	6655	No
WorkCentre®	7120/7125	No
WorkCentre®	7220/7225	No

Poodle

WorkCentre®	7425/7428/7435	Yes
WorkCentre®	7525/7530/7535/7545/7556	No
WorkCentre®	7755/7765/7775	No
WorkCentre®	7830/7835	No
WorkCentre®	7845/7855	No
WorkCentre®	7970	No
Color Models		**Vulnerable**
Xerox Color	550/560/570	No
Xerox Color	C60/C70	No
Xerox Color	C75	Yes
Xerox Color	J75	Yes
Color Models		**Vulnerable**
Versant	80	No
Versant	2100	No

Freak

Common vulnerability CVE-2015-0204. This allows SSL servers to downgrade RSA to export strength. Export strength ciphers can be broken with brute force methods. Status below is valid for the latest software version available to customers.

Monochrome Models		Vulnerable
Phaser®	3020	No
Phaser®	3052/3260	No
Phaser®	3300	No
Phaser®	3320	No
Phaser®	3600	No
Phaser®	3610	No
Phaser®	3635 MFP	No
Phaser®	4600/4620	No
Phaser®	4622	No
Phaser®	5550	No

Monochrome Models		Vulnerable
WorkCentre®	3025BI	No
WorkCentre®	3025NI	No
WorkCentre®	3210/3220	No
WorkCentre®	3215/3225	No
WorkCentre®	3315	Yes
WorkCentre®	3325	No
WorkCentre®	3550	No
WorkCentre®	3615	No
WorkCentre®	3655	No
WorkCentre®	4250	No
WorkCentre®	4260	No
WorkCentre®	4265	No
WorkCentre®	5135/5150	No
WorkCentre®	5225/5230	Yes
WorkCentre®	5325/5330/5335	Yes
WorkCentre®	5632/5638/5645/5655/5665/5675/5687	No
WorkCentre®	5735/5740/5745/5755/5765/5775/5790	No
WorkCentre®	5845/5855/5865/5875/5890	No
WorkCentre®	5945/5955	No

Monochrome Models		Vulnerable
Xerox D Series	D95A/D110/D125	Yes
Xerox D Series	D136	Yes

Color Models		Vulnerable
ColorQube®	8570/8870	No
ColorQube®	8580/8880	No
ColorQube®	8700/8900	No
ColorQube®	9201/9202/9203 CBC	No
ColorQube®	9201/9202/9203 SBC	No
ColorQube®	9301/9302/9303	No

Color Models		Vulnerable
Phaser®	6000/6010	Yes
Phaser®	6020 Windows	Yes
Phaser®	6020 Mac	Yes
Phaser®	6022 Windows	No
Phaser®	6022 Mac	No
Phaser®	6128/6128MFP	Yes
Phaser®	6280	Yes
Phaser®	6500	Yes
Phaser®	6600	No
Phaser®	6700	No
Phaser®	7100	No
Phaser®	7500	No
Phaser®	7800	No

Color Models		Vulnerable
WorkCentre®	6015 N/NI	Yes
WorkCentre®	6025 Windows	Yes
WorkCentre®	6025 Mac	Yes
WorkCentre®	6027 Windows	Yes
WorkCentre®	6027 Mac	Yes
WorkCentre®	6400	No
WorkCentre®	6505	Yes
WorkCentre®	6605	No
WorkCentre®	6655	No
WorkCentre®	7120/7125	Yes

WorkCentre®	7220/7225	No
WorkCentre®	7425/7428/7435	Yes
WorkCentre®	7525/7530/7535/7545/7556	No
WorkCentre®	7755/7765/7775	No
WorkCentre®	7830/7835	No
WorkCentre®	7845/7855	No
WorkCentre®	7970	No
Color Models		**Vulnerable**
Xerox Color	550/560/570	Yes
Xerox Color	C60/C70	Yes
Xerox Color	C75	Yes
Xerox Color	J75	Yes
Color Models		**Vulnerable**
Versant	80	Yes
Versant	2100	Yes

Logjam

Common vulnerability CVE-2015-4000. This does not properly prevent TLS downgrade of Diffie Hellman key to 512 bits. These keys can be broken with brute force methods. Note this information is limited to the strict definition of this CVE. Many security scan tools will flag this as an issue if DH keys are less than 2048 bits. Xerox is not planning to limit keys to 2048 in the near future. Status below is valid for the latest software version available to customers.

Monochrome Models		Vulnerable
Phaser®	3020	No
Phaser®	3052/3260	No
Phaser®	3300	No
Phaser®	3320	No
Phaser®	3600	No
Phaser®	3610	No
Phaser®	3635 MFP	No
Phaser®	4600/4620	No
Phaser®	4622	No
Phaser®	5550	No
Monochrome Models		**Vulnerable**
WorkCentre®	3025BI	No
WorkCentre®	3025NI	No
WorkCentre®	3210/3220	No
WorkCentre®	3215/3225	No
WorkCentre®	3315	Yes
WorkCentre®	3325	No
WorkCentre®	3550	No
WorkCentre®	3615	No
WorkCentre®	3655	No
WorkCentre®	4250	No
WorkCentre®	4260	No
WorkCentre®	4265	No
WorkCentre®	5135/5150	No
WorkCentre®	5225/5230	No
WorkCentre®	5325/5330/5335	No
WorkCentre®	5632/5638/5645/5655/5665/5675/5687	No
WorkCentre®	5735/5740/5745/5755/5765/5775/5790	No
WorkCentre®	5845/5855/5865/5875/5890	No
WorkCentre®	5945/5955	No

Monochrome Models		Vulnerable
Xerox D Series	D95A/D110/D125	No
Xerox D Series	D136	No

Color Models		Vulnerable
ColorQube®	8570/8870	No
ColorQube®	8580/8880	No
ColorQube®	8700/8900	No
ColorQube®	9201/9202/9203 CBC	No
ColorQube®	9201/9202/9203 SBC	No
ColorQube®	9301/9302/9303	No

Color Models		Vulnerable
Phaser®	6000/6010	No
Phaser®	6020 Windows	No
Phaser®	6020 Mac	No
Phaser®	6022 Windows	No
Phaser®	6022 Mac	No
Phaser®	6128/6128MFP	No
Phaser®	6280	No
Phaser®	6500	No
Phaser®	6600	No
Phaser®	6700	No
Phaser®	7100	No
Phaser®	7500	No
Phaser®	7800	No

Color Models		Vulnerable
WorkCentre®	6015 N/NI	No
WorkCentre®	6025 Windows	No
WorkCentre®	6025 Mac	No
WorkCentre®	6027 Windows	No
WorkCentre®	6027 Mac	No
WorkCentre®	6400	No
WorkCentre®	6505	No
WorkCentre®	6605	No
WorkCentre®	6655	No
WorkCentre®	7120/7125	No

WorkCentre®	7220/7225	No
WorkCentre®	7425/7428/7435	No
WorkCentre®	7525/7530/7535/7545/7556	No
WorkCentre®	7755/7765/7775	No
WorkCentre®	7830/7835	No
WorkCentre®	7845/7855	No
WorkCentre®	7970	No
Color Models		**Vulnerable**
Xerox Color	550/560/570	No
Xerox Color	C60/C70	No
Xerox Color	C75	No
Xerox Color	J75	No
Color Models		**Vulnerable**
Versant	80	No
Versant	2100	No

Additional Information

For additional information or clarification on any of the product information given here, contact your local Xerox Customer Support Centre (see table below); or visit the Xerox Website.

United States	800-835-6100		**Luxembourg**	480123
Austria	+43 1 2079000		**Netherlands**	+31 020-6563620
Belgium	+32 (2) 713 14 52 (Français), +32 (2) 713 14 53 (Nederlands)		**Norway**	+47 81 500 308
Canada	1-800-835-6100		**Portugal,**	707 200 578
Denmark	+45 70107288		**Spain**	+34 902 160 236
Finland	+358 09 693 79 666		**Sweden**	+ 46 0771 178 808
France	0825 012 013		**Switzerland**	French: 043 299 9001 German: 043 299 9000 Italian: 043 299 9002
Germany	+49 180 5004392		**UK**	+44 0870 9005501
Greece	+30 801 11 93769		**Italy**	+39 199 11 20 88

Xerox welcomes feedback on all documentation - send feedback via e-mail to: Product.Security@xerox.com.