

Digitale Infrastruktur - Bug / Feature #106

Disable SSLv2

07 July 2010 10:16 - dergringo

Status:	Closed	Start date:	07 July 2010
Priority:	Urgent	Due date:	
Assignee:		% Done:	100%
Category:		Estimated time:	0.00 hour
Target version:			
Request Type:	Feature Request		
Description			
I did a quick ssl scan on our infrastructure. And it looks like the mail services support SSLv2 which is not needed and known to be insecure. Please disable SSLv2 support and leave only SSLv3 and TLSv1 enabled.			
<pre>\$ sslscan mail.piratenpartei.ch:993 Testing SSL server mail.piratenpartei.ch on port 993</pre>			
Supported Server Cipher(s) :			
Accepted SSLv2 168 bits DES-CBC3-MD5			
Failed SSLv2 56 bits DES-CBC-MD5			
Accepted SSLv2 40 bits EXP-RC2-CBC-MD5			
Accepted SSLv2 128 bits RC2-CBC-MD5			
Accepted SSLv2 40 bits EXP-RC4-MD5			
Accepted SSLv2 128 bits RC4-MD5			
Accepted SSLv3 256 bits ADH-AES256-SHA			
Accepted SSLv3 256 bits DHE-RSA-AES256-SHA			
Rejected SSLv3 256 bits DHE-DSS-AES256-SHA			
Accepted SSLv3 256 bits AES256-SHA			
Accepted SSLv3 128 bits ADH-AES128-SHA			
Accepted SSLv3 128 bits DHE-RSA-AES128-SHA			
Rejected SSLv3 128 bits DHE-DSS-AES128-SHA			
Accepted SSLv3 128 bits AES128-SHA			
Accepted SSLv3 168 bits ADH-DES-CBC3-SHA			
Rejected SSLv3 56 bits ADH-DES-CBC-SHA			
Accepted SSLv3 40 bits EXP-ADH-DES-CBC-SHA			
Accepted SSLv3 128 bits ADH-RC4-MD5			
Accepted SSLv3 40 bits EXP-ADH-RC4-MD5			
Accepted SSLv3 168 bits EDH-RSA-DES-CBC3-SHA			
Rejected SSLv3 56 bits EDH-RSA-DES-CBC-SHA			
Accepted SSLv3 40 bits EXP-EDH-RSA-DES-CBC-SHA			
Rejected SSLv3 168 bits EDH-DSS-DES-CBC3-SHA			
Rejected SSLv3 56 bits EDH-DSS-DES-CBC-SHA			
Rejected SSLv3 40 bits EXP-EDH-DSS-DES-CBC-SHA			
Accepted SSLv3 168 bits DES-CBC3-SHA			
Rejected SSLv3 56 bits DES-CBC-SHA			
Accepted SSLv3 40 bits EXP-DES-CBC-SHA			
Accepted SSLv3 40 bits EXP-RC2-CBC-MD5			
Accepted SSLv3 128 bits RC4-SHA			
Accepted SSLv3 128 bits RC4-MD5			
Accepted SSLv3 40 bits EXP-RC4-MD5			
Rejected SSLv3 0 bits NULL-SHA			
Rejected SSLv3 0 bits NULL-MD5			
Accepted TLSv1 256 bits ADH-AES256-SHA			
Accepted TLSv1 256 bits DHE-RSA-AES256-SHA			
Rejected TLSv1 256 bits DHE-DSS-AES256-SHA			
Accepted TLSv1 256 bits AES256-SHA			
Accepted TLSv1 128 bits ADH-AES128-SHA			
Accepted TLSv1 128 bits DHE-RSA-AES128-SHA			
Rejected TLSv1 128 bits DHE-DSS-AES128-SHA			
Accepted TLSv1 128 bits AES128-SHA			
Accepted TLSv1 168 bits ADH-DES-CBC3-SHA			

Rejected	TLSv1	56 bits	ADH-DES-CBC-SHA
Accepted	TLSv1	40 bits	EXP-ADH-DES-CBC-SHA
Accepted	TLSv1	128 bits	ADH-RC4-MD5
Accepted	TLSv1	40 bits	EXP-ADH-RC4-MD5
Accepted	TLSv1	168 bits	EDH-RSA-DES-CBC3-SHA
Rejected	TLSv1	56 bits	EDH-RSA-DES-CBC-SHA
Accepted	TLSv1	40 bits	EXP-EDH-RSA-DES-CBC-SHA
Rejected	TLSv1	168 bits	EDH-DSS-DES-CBC3-SHA
Rejected	TLSv1	56 bits	EDH-DSS-DES-CBC-SHA
Rejected	TLSv1	40 bits	EXP-EDH-DSS-DES-CBC-SHA
Accepted	TLSv1	168 bits	DES-CBC3-SHA
Rejected	TLSv1	56 bits	DES-CBC-SHA
Accepted	TLSv1	40 bits	EXP-DES-CBC-SHA
Accepted	TLSv1	40 bits	EXP-RC2-CBC-MD5
Accepted	TLSv1	128 bits	RC4-SHA
Accepted	TLSv1	128 bits	RC4-MD5
Accepted	TLSv1	40 bits	EXP-RC4-MD5
Rejected	TLSv1	0 bits	NULL-SHA
Rejected	TLSv1	0 bits	NULL-MD5

Prefered Server Cipher(s) :

SSLv2	168 bits	DES-CBC3-MD5
SSLv3	256 bits	ADH-AES256-SHA
TLSv1	256 bits	ADH-AES256-SHA

History

#1 - 19 July 2010 15:35 - Anonymous

- Status changed from New to Closed
- % Done changed from 0 to 100

Done.

#2 - 09 November 2010 14:30 - dergringo

- Project changed from 8 to 16
- Category deleted (1)