

Forum:[Hack Forums](#)

Thread: [SSL 2.0 deprecated protocol?](#)

Abdilo - April 16, 2012, 9:27 pm

Hey guys,

I found a SSL 2.0 deprecated protocol (High Level Threat) in a popular website.

Can this be exploited?

Pwease tell me :D

Code The remote service accepts connections encrypted using SSL 2.0, which suffers from several cryptographic flaws and has been deprecated.

Libyano - April 16, 2012, 9:32 pm

Yes. I'm studying SSL, encoding systems and such (the logical/mathematical way) it's really not that hard.

Use this book, it give you everything you need (it's the same book we use as a reference):

Computer Security Series

Security Technologies

For the World Wide Web

Second edition

~Rolf Oppliger.

Abdilo - April 16, 2012, 9:34 pm

(Apr 16, 2012 09:32 PM)Libyano Wrote: [\[CITE\]](#) Yes. I'm studying SSL, encoding systems and such (the logical/mathematical way) it's really not that hard.

Use this book, it give you everything you need (it's the same book we use as a reference):

Computer Security Series

Security Technologies

For the World Wide Web

Second edition

~Rolf Oppliger.Ok,

So this is exploitable what can I do with it? can I steal stuff or upload stuff?

Libyano - April 16, 2012, 10:04 pm

(Apr 16, 2012 09:34 PM)Notavirus Wrote: [\[CITE\]](#) Ok,

So this is exploitable what can I do with it? can I steal stuff or upload stuff?

Hi & sorry for the late reply, didn't notice it.

Yes once you crack it down you can manipulate it anyway you want. You can have total access to it. You can change what the user is viewing, etc.

Look at pages 128-141. And chapters 6 & 7.

Abdilo - April 16, 2012, 10:48 pm

(Apr 16, 2012 10:04 PM)Libyano Wrote: [\[CITE\]](#) Hi & sorry for the late reply, didn't notice it.

Yes once you crack it down you can manipulate it anyway you want. You can have total access to it. You can change what the user is viewing, etc.

Look at pages 128-141. And chapters 6 & 7. Fuck YEAH! ? now I will have a shit load of emails, passwords, credit cards and more! ?