How to avoid the SSL Poodle attack

Applies to VoipNow Professional 2.5 and VoipNow 3.0.0 - 3.0.5!

There seems to be a vulnerability in the SSLv3 protocol, which is described in CVE-2014-3566 (short name 'POODLE'). All implementations of SSLv3 are affected.

This vulnerability allows a man-in-the-middle attacker to decrypt SSL traffic. More details can be found here.

Step-by-step guide

To verify if you are vulnerable, please run:

1. `curl -v3 -X HEAD https://www.example.com`
2. If you see "`curl: (35) SSL connect error`", then you are not vulnerable. If you have a normal SSL connection, this means you are vulnerable.

To avoid being exploited, please run:

1. `wget https://raw.githubusercontent.com/4psa/voipnowpatches/master/sslpoodlefix.sh`
2. `sh sslpoodlefix.sh`

Related articles

- How to install a LetsEncrypt SSL certificate in VoipNow
- How to avoid the SSL Poodle attack
- How to change the SSL certificate in VoipNow
- How to change my 4PSA DNS Manager HTTP server SSL certificate