Fixing Poodle Vulnerability

The POODLE vulnerability, which stands for Padding Oracle On Downgraded Legacy Encryption, is a vulnerability in the SSL 3.0 protocol that allows an attacker to exploit the way in which the protocol handles padding to extract plaintext secrets from encrypted communications.

To remediate the POODLE vulnerability, you generally want to disable SSL 3.0 in your environment, regardless of whether you're using a server or a client

1. **Disabling SSL 3.0 on Web Servers**

For Apache:

1. Edit your Apache configuration file, typically found at `/etc/httpd/conf/httpd.conf` or `/etc/apache2/apache2.conf`.
2. Locate the SSLProtocol directive and change it to:

```
SSLProtocol All -SSLv2 -SSLv3
```

3. Save the file and restart the Apache server:

```
sudo service apache2 restart
```

For Nginx:

1. Edit your Nginx configuration file, typically found at `/etc/nginx/nginx.conf`.
2. In the `ssl` configuration block, locate or add the `ssl_protocols` directive and set:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

3. Save the file and restart Nginx:

```
sudo service nginx restart
```

2. **Disabling SSL 3.0 on Mail Servers**

1. Edit the Postfix configuration, typically `/etc/postfix/main.cf`.

2. Find or add the `smtpd_tls_mandatory_protocols` and `smtp_tls_mandatory_protocols` lines:

```
smtpd_tls_mandatory_protocols=!SSLv2, !SSLv3
smtp_tls_mandatory_protocols=!SSLv2, !SSLv3
```

3. Save and restart Postfix:

```
sudo service postfix restart
```

3. **Testing for Vulnerability**

After making changes, always test to make sure that SSL 3.0 is indeed disabled. Perform a rescan from brandsek to check whether the security issue has been fixed.

Additionally, for manual testing, you can use the following OpenSSL command:

```
openssl s_client -connect yourdomain.com:443 -ssl3
```

If you see a handshake failure, it likely indicates that SSL 3.0 has been successfully disabled.

Note: Ensure you always have backups of any configurations before making changes and always test your changes in a staging or test environment before deploying to production.

Revision #1
Created 19 October 2023 14:24:15 by Admin
Updated 20 October 2023 01:07:28 by Admin