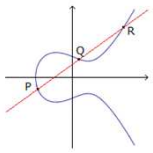
IBM MQ SSL : Problèmes & Solutions



Luc-Michel Demey
LMD@demey-consulting.fr
+33 6 08 755 655

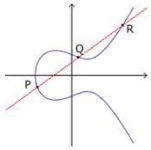
Version 1.00 - Décembre 2014

Vulnérabilités SSL 2014

- Heartbleed

- Poodle

- Elliptic Curve



Heartbleed

- Vulnérabilité logicielle dans le code de **OpenSSL**
- Présente depuis 03/2012 (version 1.0.1)
- Découverte en 03/2014
- Publiée en 04/2014 : CVE-2014-0160
- Corrigée en version 1.0.1g +

Impacts

- Récupération par le correspondants de blocs mémoire
- Le contenu de ces blocs peut être sensible …
  - Mots de passe, clés de sécurité SSL
- … ou pas
- A priori exploité
- Impacts sur sites web, routeurs, applications
  - Cisco, Juniper
  - Android 4.1.1
  - Appliances
  - Tous les runtimes utilisant OpenSSL

Impacts IBM

- WAS, IHS, WMQ/IIB et IBM MQ non vulnérables
- IBM Java JSSE non vulnérable
- Clients MQTT vulnérables
  - Support Pac MAT1 - WebSphere MQ client for HP Integrity NonStop Server
  - Support Pac MA9B - IBM Mobile Messaging and M2M Client Pack - Eclipse Paho MQTT C Client libraries for Linux & Windows platforms only

Poodle

- Poodle : Padding Oracle On Downgraded Legacy Encryption
- Faille de sécurité dans l'architecture du protocole SSL 3.0
- Présente depuis … 15 ans ?
- Publiée en 10/2014 : CVE-2014-3566
- Non corrigeable → passer en TLS

Impacts

- Permet de forcer la négociation d'un lien SSL/TLS en SSL
- Facilite les attaques type *man-in-the-middle*
- Permet le décryptage progressif des flux échangés
- Tous les systèmes autorisant SSL v3 sont à priori impactés

Impact IBM

- Nombreux produits impactés, y compris WMQ :
  - Domino, Notes, WAS, IHS, …
- Mais uniquement si utilisation de ciphers SSL
- IBM MQ :
  - Pas de négociation de cipher possible
  - Donc pas d'impact si utilisation d'un cipher TLS

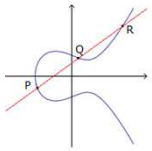
Solutions WMQ

- S'assurer que les cipher utilisés sur chaque canal ne soient pas de type « SSL v3 »
- Exemples de cipher SSL V3 :
  - AES_SHA_US, RC4_SHA_US, RC4_MD5_US
  - TRIPLE_DES_SHA_US, DES_SHA_EXPORT1024
  - RC4_56_SHA_EXPORT1024, RC4_MD5_EXPORT
  - RC2_MD5_EXPORT, DES_SHA_EXPORT
  - NULL_SHA, NULL_MD5
  - FIPS_WITH_DES_CBC_SHA, FIPS_WITH_3DES_EDE_CBC_SHA
- Note : L'activation de FIPS empêche l'utilisation des ciphers SSL v3

Activation de FIPS

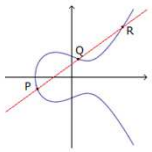
- L'activation de FIPS empêche l'utilisation des ciphers SSL V3
- Mais empêche également d'autres ciphers :
  - ECDHE_ECDSA_NULL_SHA256
  - ECDHE_ECDSA_RC4_128_SHA256
  - ECDHE_RSA_NULL_SHA256
  - ECDHE_RSA_RC4_128_SHA256
  - TLS_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_WITH_NULL_SHA256
  - TLS_RSA_WITH_RC4_128_SHA256
- Activation (niveau QMGR) : ALTER QMGR SSLFIPS(YES)

Elliptic Curve



- Chiffrement par « courbes elliptiques » (ECC)
- Clés plus courtes que via factorisation type RSA, sécurité équivalente ou supérieure
- Une clé de 200 bits en EC est équivalente à une clé de 1024 en RSA
- Utilisé dans les ciphers IBM MQ :
  - ECDHE_ECDSA_NULL_SHA256
  - ECDHE_ECDSA_RC4_128_SHA256
  - ECDHE_RSA_NULL_SHA256
  - ECDHE_RSA_RC4_128_SHA256

Vulnérabilité Elliptic Curve



- « Timer attack » permettant en théorie de déduire une partie de la clé
- Publiée le 04/11/2014 (CVE-2014-0076)
- Impacte IBM GSKit, donc WMQ :
  - IBM WebSphere MQ 8.0, including all maintenance levels.
  - IBM WebSphere MQ 7.5, including all maintenance levels.
  - IBM WebSphere MQ 7.1, including all maintenance levels.
  - IBM WebSphere MQ 7.0.1, maintenance levels from 7.0.1.4

Bilan pour WMQ

- Heartbleed : pas d'impact
- Poodle :
  - Éviter les ciphers en SLL v3
  - Pas d'impact en pratique si TLS
  - Possibilité d'activer FIPS
- ECC :
  - Pas d'impact en pratique
  - FIPS n'autorise pas ECC

Bilan pour WMQ

- Solution de facilité : Activer FIPS
  - Avec précaution
- Choisir un cipher TLS 1.0 ou 1.2
- Un bon choix : TLS_RSA_WITH_AES_128_CBC_SHA
  - Disponible de MQ 7.0 à MQ 8.0
  - TLS 1.0 / SHA1 / AES128
  - Certifié FIPS
- TLS 1.2 en MQ 8.0 permet le « multi-certificat »

Conclusion

- Pour se protéger des « pirates » : pas de cipher de type « SSL »
- Pour se protéger des audits : activer FIPS

Sources

- https://fr.wikipedia.org/wiki/Heartbleed
- https://www-304.ibm.com/connections/blogs/PSIRT/entry/openssl_heartbleed_cve_2014_0160
- CVE-2014-0160 : http://www-01.ibm.com/support/docview.wss?uid=swg21669839
- https://fr.wikipedia.org/wiki/POODLE
- CVE-2014-3566 : http://www-01.ibm.com/support/docview.wss?uid=swg21687173
- https://www-304.ibm.com/connections/blogs/PSIRT/entry/sslv3_vulnerable_to_cve_2014_3566_poodle_attack
- https://fr.wikipedia.org/wiki/Cryptographie_sur_les_courbes_elliptiques
- CVE-2014-0076 : http://www-01.ibm.com/support/docview.wss?uid=swg21688949
- Security Bulletin IBM : http://www-01.ibm.com/support/docview.wss?uid=swg21687433&myns=swgws&mynp=OCSSFKSJ&mync=E
- Ciphers MQ V7.0.1 : http://www-01.ibm.com/support/knowledgecenter/SSFKSJ_7.0.1/com.ibm.mq.csqzaw.doc/ja34740_.htm?lang=fr
- Ciphers MQ V8.0 : http://www-01.ibm.com/support/knowledgecenter/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q014260_.htm
- FIPS : http://www-01.ibm.com/support/knowledgecenter/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q010140_.htm
- Images wikimedia

Page blanche intentionnellement