IBM Software

AVP Expert Call Series

Exclusively for AVP Clients

Security Question & Answer Session

Bill O'Donnell
IBM Systems Middleware Security Compliancy Officer
WebSphere Foundation Security Architect

Brett Ostrander
WebSphere Application Server Level 2 Security Team Lead

Toll-Free: 1-888-426-6840
PassCode: 6401181#

August 20, 2015

About the Expert Panel

- Bill O'Donnell bill.odonnell@us.ibm.com

  - IBM Systems Middleware Security Compliancy Officer and WebSphere Foundation Security Architect (Austin Labs).
  - Security Compliancy officer for IBM Middleware Products for Cloud™ and IBM Software. Ensure IBM compliancy for a wide range of security standards and ensuring teams are following secure engineering best practices and Security Vulnerability handlement.
  - Security Architect for WebSphere Application Server.
  - http://www.ibm.com/developerworks/websphere/zones/was/security/

- Brett Ostrander bretto@us.ibm.com

  - WebSphere Application Server Level 2 Security Team Lead.
  - Subject Matter Expert for Security/SSL.
  - 13 years of experience in WebSphere and 16 years in support.
  - Certified in WebSphere V6, V7 and V8.

© 2015 International Business Machines Corporation

Best Practices for Addressing Weaknesses in SSL

- Move away from any Server Certificate that digitally signed using SHA1. Browser Vendors plan on blocking in 2016.
  - Certificates will need to be converted to use SHA256withRSA in WebSphere Application Server.
  - http://www-01.ibm.com/support/docview.wss?uid=swg21959568
- Server Certificate must be using 2048 or higher encryption keys.
- Move to TLS 1.2 Protocol
  - SSL Handshake key exchange uses a stronger SHA2 based Cipher.
  - Offers Ciphers based on SHA2 and higher.
  - Good news, seeing a trend where Software Vendors are adopting TLS 1.2.
  - Be aware, while all major browser vendors now support TLS 1.2, the older version do not or they have TLS 1.2 disabled by default.
- Using SHA2 (or higher) or use Elliptic Curve (ECC) based Ciphers.
- **IBM Strongly recommends that customer running WAS 6.1 and IHS 7.0 need move to WAS/IHS 8.5 given the stronger encryption standards are not supported.**

© 2015 International Business Machines Corporation

Questions Received in Advance

1. Can you review the security implications of staying on WAS v6.1, and why should we move to a later release?
2. There are a number of cross site scripting vulnerabilities fixed in the admin console. Are there any Best Practices to avoid these issues until Fix Packs are applied?
3. What is the current assessment on how vulnerable CBC ciphers are to Beast? Since this is a client side vulnerability and many web sites may not be able to enforce what clients can connect, should CBC ciphers be used? If CBC ciphers should not be used, will they be removed from IHS and WAS default cipher lists?
4. TLS 1.1 is vulnerable to POODLE, is there going to be an update to remove TLS 1.0?
5. Are there any performance impacts to using larger encryption keys?
6. Which are the best performing high strength ciphers?
7. How often should LTPA keys be changed? What are the implications of changing the keys? Should servers be restarted if the keys are changed?

© 2015 International Business Machines Corporation

What are Your Questions?

To ask a question hit *6 to unmute your line.
You may post your question in the chat as well.
Please limit your questions to two at a time, additional questions can be taken at the end or offline.

This session is being recorded and will be available on our Expert Call Series technote. Your AVP team will send out an email with the replay information.

http://www-01.ibm.com/support/docview.wss?uid=swg27038322

© 2015 International Business Machines Corporation

Stay tuned for additional presentations as part of the AVP Expert Call Series!

Please provide feedback to your AVP team on today's session and if interested in further deep-dive topics:

Security Vulnerabilities

Downgrade: Poodle, Freak
Ciphers: Beast, Bar Mitzvah, Log Jam
AVP Vulnerability detection script

Security Basics

Background on SSL / TLS
Basic Security Vocabulary
Common Issues and Misconceptions
Cryptograph Basics

Advanced Security Topics

SSL / PKI Hints and Caveats
Certificates
Certificate Authorities
Keystores

© 2015 International Business Machines Corporation