FAQ for OfficeScan (OSCE) 10.6 Service Pack (SP) 3 Critical Patch (CP) 5712r1

1. What is the purpose of OfficeScan (OSCE) 10.6 Service Pack (SP) 3 Critical Patch (CP) 5712r1?

   Trend Micro is constantly monitoring and improving its technology as part of our commitment to providing the best protection possible for our customers. Trend Micro's Smart Scan file reputation is one of the key pieces of technology that enables customers to utilize the power of the cloud for pattern detection.

   One component of Smart Scan, the Smart Query Filter (BF.ptn), helps Smart Scan clients filter out unnecessary traffic to the Smart Protection Server, helping to conserve overall network bandwidth. The size of BF.ptn is directly proportional to the file size of the overall Smart Scan Pattern, which continues to grow quite rapidly due to increased threats in recent months. The result of this rapid growth is that BF.ptn will need to update and redeploy a balanced version to Smart Scan clients.

   Background and Detail

   BF.ptn is periodically and automatically re-optimized by the Smart Protection Server utilized by OfficeScan. Following this re-optimization process, BF.ptn is then redeployed to Smart Scan clients.

   Based on the algorithm controlling BF.ptn optimization and current rate of pattern updates, Trend Micro is estimating that BF.ptn will increase in substantially in size sometime during the months of January, February or March, **2016**. Unfortunately, due to the complexity of the algorithm, it is not possible to pinpoint the exact date the update will occur, but it will only happen once during this timeframe.

   Affected Versions and Managing Potential Impact

   The BF.ptn update will be transparent and a largely uneventful occurrence for most of Trend Micro's customers.

   However, companies who have deployed OfficeScan 10.6 that have bandwidth concerns or sensitivity to the impact of a 27MB one-time update to all Smart Scan clients are encouraged to take some preliminary steps before the January-March, 2016, update; the most important being the application of OfficeScan 10.6 Service Pack 3 Patch 1 Critical Patch 5712r1, which includes some critical updates to enhance some of the core component of Smart Scan in OfficeScan 10.6.

   This update will eliminate the need for the deployment of a BF.ptn update in the future. Other benefits for this Smart Scan Enhancement Critical Patch include significantly reducing the number of queries needed to effective use the Smart Protection Server, which effectively cuts down on false positives, as well reducing the overall memory footprint on OfficeScan clients.

2. Who can install OSCE 10.6 SP 3 CP 5712r1?
   All OSCE 10.6 customers (10.6 GM build, SP1, SP2, SP3 or higher) are advised to apply this CP. Alternatively, customers can also upgrade to OSCE 11, which already includes this.

3. When should customers apply this Critical Patch?
   Customers need to apply this Critical Patch before January 2016.

4. What are steps needed to install this OSCE 10.6 SP3 CP 5712r1?
   For customers using the following build:
   - OSCE 10.6 GM Build
   - OSCE 10.6 SP1 or higher (i.e. OSCE 10.6 SP1 Patch x)
   - OSCE 10.6 SP2 or higher (i.e. OSCE 10.6 SP2 Patch x)

   a. First, download and install OSCE 10.6 Service Pack 3
   b. Then, follow the steps below (For Customers using OSCE 10.6 SP3) to install the Critical Patch

   For Customers using OSCE 10.6 SP3:

   a. If you are using Standalone Smart Protection Server (SPS) version 2.x, upgrade to SPS 3.0
   b. Install OSCE 10.6 SP3 Patch 1.1
   c. Install Critical Patch 5495
   d. Install OSCE 10.6 SP3 Patch 2 (optional, but recommended to keep OSCE up-to-date)
   e. Lastly, Install OSCE 10.6 SP3 CP 5712r1

   NOTE: Before applying the next patch / Critical Patch, please make sure all clients are up-to-date. If you want to control the deployment of the Patch/CP, please open the OSCE console and go to Networked Computers | Client Management | Settings | Privilege and Other Settings | Other Settings |Update Settings and enable or disable the “Clients can update components but not upgrade the client program or deploy hot fixes”. Enable this feature before applying the Patch/CP. Then, install the Patch/CP. Then, disable this feature again after installing the Patch/CP. It is strongly recommended that you schedule / stagger the deployment of this Critical Patch to OSCE clients to avoid any high network bandwidth usage. The one time deployment of new smart scan pattern (crcz.ptn) is approximately 20+ MB.

   For Customers using OSCE 10.6 SP3 Patch 1 or OSCE 10.6 SP3 Patch 1.1:

   a. If you are using Standalone Smart Protection Server (SPS) version 2.x, upgrade to SPS 3.0
   b. Install Critical Patch 5495
   c. Install OSCE 10.6 SP3 Patch 2 (optional, but recommended to keep OSCE up-to-date)
   d. Lastly, Install OSCE 10.6 SP3 CP 5712r1

   NOTE: Before applying the next patch / Critical Patch, please make sure all clients are up-to-date. If you want to control the deployment of the Patch/CP, please open the OSCE console and go to Networked Computers | Client Management | Settings | Privilege and Other Settings | Other Settings |Update Settings and enable or disable the “Clients can update components but not upgrade the client program or deploy hot fixes”. Enable this feature before applying the Patch/CP. Then, install the Patch/CP. Then, disable this feature again after installing the Patch/CP. It is strongly recommended that you schedule / stagger the deployment of this Critical Patch to OSCE clients to avoid any high network bandwidth usage. The one time deployment of new smart scan pattern (crcz.ptn) is approximately 20+ MB.

For Customers using OSCE 10.6 SP3 Patch 2:

a. If you are using Standalone Smart Protection Server (SPS) version 2.x, upgrade to SPS 3.0
b. Install OSCE 10.6 SP3 CP 5712r1

NOTE: If you want to control the deployment of the Critical Patch, please open the OSCE console and go to Networked Computers | Client Management | Settings | Privilege and Other Settings | Other Settings |Update Settings and enable or disable the "Clients can update components but not upgrade the client program or deploy hot fixes". Enable this feature before applying the CP. Then, install the CP. Then, disable this feature again after installing the CP. It is strongly recommended that you schedule / stagger the deployment of this Critical Patch to OSCE clients to avoid any high network bandwidth usage. The one time deployment of new smart scan pattern (crcz.ptn) is approximately 20+ MB.

5. What happens if customers don't apply this Critical Patch before the deadline?
   All OSCE smart scan clients will download a one-time 27 MB full BF.ptn pattern update.

6. What are the benefits of applying this Critical Patch?
   - Eliminate the need for the deployment of a one-time full BF.ptn update in the future.
   - Significantly reducing the number of queries needed to effective use the Smart Protection Server, which effectively cuts down on false positives.
   - Reducing the overall memory footprint on OfficeScan clients.

7. What happens when this Critical Patch is deployed?
   - OSCE clients will download the Critical Patch (including the CRCz.ptn) via program updates from the OSCE server. This is a one-time download of CRCz.ptn from the OSCE server. File size of CRCz.ptn is approximately 20 MB. Moving forward, any incremental updates of CRCz.ptn will be downloaded from integrated Smart Protection Server or Standalone Smart Protection Server. The CRCz.ptn replaces the BF.ptn used in smart scan pattern. Below is the file size of the Critical Patch (including CRCz.ptn) that will be deployed to OSCE clients:
     - For 32-bit client : 37.2 MB
     - For 64-bit client : 44.2 MB

   NOTE: To minimize network traffic, it is highly recommended to stagger the deployment of this critical patch.

8. After installing the Critical Patch, for customers using Apache or IIS web server, what ports will be used for communication between the OSCE clients and the integrated Smart Scan Protection Server?
   Apache web server will use the following ports for Smart Scan queries:
   - File Reputation (HTTP): 8082
   - File Reputation (HTTPS): 4345
   - Web Reputation (HTTP): 5274

   Note: If these ports have been used by other applications, it can be changed to other ports during installation of the Critical Patch.

   IIS web server will use existing ports to handle Smart Scan queries

   For Virtual Web site
   - FRS HTTP: 8082 / SSL: 4345
   - WRS HTTP: 5274

For Default Web Site

- FRS HTTP: 80 / SSL: 443
- WRS HTTP: 80

9. Is Standalone Smart Scan Protection Server v3.0 compatible with OSCE 10.5, 10.6 (with or without the Critical Patch installed) or 11 clients?
   Yes, Standalone Smart Scan Protection Server v3.0 is backward compatible. It supports OSCE versions 10.5, 10.6 (with or without the Critical Patch Installed) or 11.0 clients.

10. Is OSCE 10.6 SP3 Patch 1 Critical Patch 5712r1 compatible with Trend Micro Control Manager (TMCM) ?
    Yes, the following TMCM builds are compatible.
    - TMCM 5.5 SP1 Patch 5 and above
    - TMCM 6.0 SP1 and above

11. My OfficeScan server is configured to utilize conventional scan only (NOT smart scan), should I still apply this Critical Patch?
    OfficeScan customers using purely conventional scan may opt to delay applying the Critical Patch. However, it is still advisable to apply the Critical Patch as to take full advantage of the new smart scan architecture if and when you decide to enable this feature. Also, for customers using OSCE 10.6 Service Pack 3 and above, it is a pre-requisite to apply the Critical Patch if an OSCE hotfix is requested.

12. I am using OSCE 10.6 Service Pack 3 or above build and need to apply an OSCE hotfix. Do I need to apply the Critical Patch first?
    For customers who are using OSCE 10.6 Service Pack (SP) 3 and above (i.e. OSCE 10.6 SP3, OSCE 10.6 SP3 Patch1, OSCE 10.6 SP3 Patch 2), it is a pre-requisite to apply the Critical Patch before applying the OSCE hotfix.

13. I have installed the Critical Patch 5712 before Jan 23, 2015. Do I need to reapply it?
    Yes, please download and reapply the repack Critical Patch 5712r1 on the OSCE server. The reason to reapply the repack of Critical Patch is to address the issue where the OfficeScan integrated Smart Protection Server 3.0 may download the full CRCZ pattern file from the File Reputation ActiveUpdate server. As a result, the server uses up more bandwidth while updating pattern files.

14. What are the new enhancements on the repack of Critical Patch 5712r1?
    - After applying OfficeScan 10.6 Service Pack 3 Patch 1 Critical Patch 5712, OfficeScan clients will schedule a download of the CRCZ pattern from the iSPS 3.0 or standalone Smart Protection Server (SPS) 3.0. The download task may remain in processing status for a period of time during which the computer's performance may slow down while opening applications. This occurs because the Smart Scan Pattern is not locally available to filter FRS queries. As a result, FRS queries pile up on iSPS and SPS.
      - This Critical Patch 5712r1 enhances the pattern deployment mechanism so that the latest full CRCZ pattern will be deployed together with the OfficeScan binaries.

- The integrated Smart Protection Server 3.0 may download the full CRCZ pattern file from the File Reputation ActiveUpdate server even when the update is in the incremental range. As a result, the server uses up more bandwidth while updating pattern files.
    - This Critical Patch 5712r1 ensures that the OfficeScan Smart Protection Server downloads only the incremental CRCZ pattern file when the update is in the incremental range.