CROSS-SYSTEM SECURITY VALIDATION USING SAP SOLUTION MANAGER 7.1
SIS262
Exercises / Solutions
Frank Buchholz, Active Global Support Security Services
Software security remains a critical topic of interest to all companies and to the information technology industry. The security of a specific system thereby also significantly depends on the secure configuration of this system.

With **Configuration Validation** within SAP Solution Manager, SAP offers a tool to validate various kinds of software configuration items. This helps to standardize and harmonize configuration items within the ABAP and Java world cross system, using a single configuration item repository within SAP Solution Manager.

In this hands-on session participants learn to use configuration validation templates with typical use cases in the space of Security Validation. The basic set-up of Configuration Validation is explained step by step and described for typical reporting scenarios. As the use case, a typical software level and parameter validation scenario will be implemented. We'll use the latest options of SAP Solution Manager 7.1 to define a target system which exactly matches the strong requirements of many corporate security policies.

**Contents**

01 View Security Chapter of EarlyWatch Alert ............................................................................ 3
02 View Security Optimization Service Report ............................................................................... 7
03 Create Target System for Configuration Validation ................................................................. 10
04 Maintain Target System for Configuration Validation .............................................................. 14
   Config Store STANDARD_USERS ......................................................................................... 15
   Config Store AUTH_PROFILE_USER ................................................................................. 15
   Config Store SICF_SERVICES ......................................................................................... 16
   Config Store SAP_KERNEL .............................................................................................. 16
   Config Store MS_SECINFO .............................................................................................. 16
   Config Store GW_REGINFO ............................................................................................ 17
   Config Store GW_SECINFO ............................................................................................ 17
   Config Store GLOBAL ................................................................................................... 17
   Config Store ABAP_NOTES ........................................................................................... 18
   Config Store ABAP_INSTANCE_PAHI .............................................................................. 19
05 Create Comparison System List for Configuration Validation ....................................................... 21
06 Show Configuration Validation Report ..................................................................................... 22
07 Show Configuration Validation Report for Security Notes ............................................................ 26
01 View Security Chapter of EarlyWatch Alert

During this exercise we check the settings of critical profile parameters using the EarlyWatch Alert report. This report shows strong recommendations from SAP for one single system.

Logon to the SAP Solution Manager system and start the ABAP WebDynpro application SAP Solution Manager Work Center

Start the SAP Solution Manager Work Center using the link in the Easy Access Menu (or using transaction SOLMAN_WORKCENTER) and navigate to the tab “SAP Engagement and Service Delivery”
1. In the SAP Solution Manager Work Center navigate to the EarlyWatch Alert on the tab “SAP Engagement and Service Delivery”
2. Select “Reports”
3. Select “EarlyWatch Alert”
4. Ensure, that you are using the solution “SAP Security Check” (expand and use the filter to change it)
5. Start search (if not automatically done)
6. Select a green, yellow or red EarlyWatch Alert report

Scroll down to view the details.
You can notice a couple of alerts concerning security related topics, too.
1. Switch to tab "Attachments"
2. Open the EarlyWatch Alert report (the reports gets downloaded to the PC and opened with Word)

Scroll down to the chapter concerning security:

11 Security

Critical security issues were found in your system. See the information in the following sections.

11.1 SAP Security Notes: ABAP and Kernel Software Corrections

Software corrections from SAP Security Notes are missing in this system. Your system is probably exposed to security threats.

Recommendation: Apply SAP Security Notes that are relevant to your system. A complete list of SAP Security Notes, including Security HotNews, is available on SAP Service Marketplace, at https://service.sap.com/securitynotes. The RSENCOTE tool in transaction ST13 provides a list of missing SAP Security Notes. RSENCOTE covers SAP Security HotNews with software-related corrections for ABAP or kernel, and a selection of other SAP Security Notes. For more information, see SAP Note 8888888.

In the Security Notes list at the SAP Service Marketplace location above, the "Automatic check in EWA" flag (last column) identifies those SAP Security Notes for which the implementation is fully checked by the RSENCOTE tool.

11.2 Default Passwords of Standard Users

Standard users have default passwords.

Recommendation: Run report RSUR003 in each client, to check the use of default passwords by standard users. Ensure that users SAPCPCIC and EARLYWATCH have non-default passwords in all clients.

For more information, see http://help.sap.com/saphelpnw70/helpdata/EN/3e/cdacbccd411d3a6510000e835363f/frameset.htm["Protecting Standard Users"] either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

Make sure that the standard password for user TMSADM has been changed in client 000, and delete this user in any other client. SAP Note 1414256 describes a support tool to change the password of user TMSADM in all systems of the transport domain.

SAP Note https://service.sap.com/sap/support/notes/1552894[1552894] shows how to update the report RSUSR003 to show the status of user TMSADM.
You see that some chapters deal with profile parameters settings. Here is a typical list of profile parameters which is listed in the EarlyWatch Alert report:

<table>
<thead>
<tr>
<th>Profile Parameter</th>
<th>Actual value</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/no_automatic_user_sapstar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_lng</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_digits</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_lowercase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_uppercase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/password_max_idle_initial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>gw/acl_mode</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How could you check more security relevant parameters?
⇒ see next chapter about **Security Optimization Service**

How could you check this for many systems automatically?
⇒ see next chapter about **Configuration Validation**

How could you validate your Company Security Policy?
⇒ see next chapter about **Configuration Validation**
02 View Security Optimization Service Report

During this exercise we check the settings of critical profile parameters using the Security Optimization Service report. This report shows strong recommendations from SAP for one single system.

Start the SAP Solution Manager Work Center using the link in the Easy Access Menu (or using transaction SOLMAN_WORKCENTER) and navigate to the tab “SAP Engagement and Service Delivery”
1. In the SAP Solution Manager Work Center navigate to the EarlyWatch Alert on the tab “SAP Engagement and Service Delivery”
2. Ensure that you view “Services”
3. Ensure, that you are using the correct solution (expand and use the filter to change it)
4. Open the session for your system (see “Scope”)
5. Select the session
6. Switch to tab “Attachments” on the details box
7. Open the SOS report (the reports gets downloaded to the PC and opened with Word)
Within the report scroll down to view the password policy checks.

5.1 Password Logon Is at Least Partly Allowed (0139)

Logging on with passwords is at least partially allowed. Allow all users to log on with their password (login/disable_password_logon = 0), or at least special groups that are described in the parameter login/password_logon_usergroup.

**Recommendation:**
If you are not using Single Sign-On (SSO), at least think about implementing an SSO solution. To further increase the security of your systems, prevent users from logging on with their passwords.

5.2 Password Policy

If password login is allowed for specific instances only, the password policy is checked only for these instances.

5.2.1 Password Complexity

5.2.1.1 Minimum Password Length

<table>
<thead>
<tr>
<th>Parameter: login/min_password_len</th>
<th>Current Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>wdfbmt0698_M38_10</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

The current system settings allow a minimum password length less than 8 characters. This allows weak passwords. Attackers may successfully recover those passwords and exploit this to gain unauthorized access to the system.

**Recommendation:** Use a minimum value of 8 for the profile parameter login/min_password_len.

5.2.1.2 Character Category Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Instance</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_digits</td>
<td>wdfbmt0698_M38_10</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td>wdfbmt0698_M38_10</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_lowercase</td>
<td>wdfbmt0698_M38_10</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_uppercase</td>
<td>wdfbmt0698_M38_10</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td>wdfbmt0698_M38_10</td>
<td>0</td>
</tr>
</tbody>
</table>

**Evaluation Risk - Medium**

SAP provides options to enforce complex passwords. Find the current settings of the corresponding profile parameters in the table.

**Recommendation:** Enforce a minimum of 3 independent character categories using the corresponding profile parameters. For more information, see SAP Note 862989 and the section Profile Parameters for Logon and Password (Login Parameters) either on SAP Help Portal or in the SAP NetWeaver AS ABAP Security Guide.

How could you check this for many systems automatically?

⇒ see next chapter about **Configuration Validation**

How could you validate your Company Security Policy?

⇒ see next chapter about **Configuration Validation**
03 Create Target System for Configuration Validation

During this exercise we check the settings of critical system parameters using the Configuration Validation application within the SAP Solution Manager.

The first step is to define a **Target System** which contains the target values for system settings. Such a Target System should represent the requirements of your Corporate Security Policy / Security Baseline.

Start the SAP Solution Manager Work Center using the link in the Easy Access Menu (or using transaction SOLMAN_WORKCENTER) and navigate to the tab "Change Management".
Start the **SAP Solution Manager Work Center** within SAP Solution Manager.

1. Navigate to “**Change Management**”
2. Execute “**Configuration Validation**”
1. Ensure that you are in create mode.

2. First we have to select a **Source System** which gives us proposals about **Config Stores** and configuration values which could be part of our **Target System**. Display the existing Source Systems.

1. Select any (dummy) source system, e.g. your system. You see a list of available Configuration Stores.

2. However, as we know that there exist a special template for security validation we do not select the Config Stores manually but choose the function **“Create with Template”**.
1. Enter a Target System Id
   Choose a unique name
   Enter a description

2. Select the SAP template **0SEC.NEW**

3. Scroll down and create the Target System

You get a confirmation message. Close the window.
04 Maintain Target System for Configuration Validation

During this exercise we check the settings of critical system parameters using the Configuration Validation application within the SAP Solution Manager.

The second step is to maintain the **Target System** which contains the target values for system settings. Such a Target System should represent the requirements of your Corporate Security Policy / Security Baseline.

1. Switch to edit mode.

2. You do not see the new Target System yet, therefore you have to use the function “**Display all**”.

![Target System Maintenance](image)
Select your Target System.
Now you can view and maintain the target values of the Config Stores of this Target System.

Examples (select a store to view the details):

**Config Store STANDARD_USERS**
The template values describe that any standard user has to have a changed password and that user SAP* has to exist in all clients.
No change required

```
Target System : SEC_00 / Store Name : STANDARD_USERS

<table>
<thead>
<tr>
<th>CLIENT</th>
<th>USER</th>
<th>PASSWORD_STATUS</th>
<th>EXISTS</th>
<th>LOCKED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(Not equal) DEFAULT</td>
<td>(Ignore) X</td>
<td>ignore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Not equal) DEFAULT</td>
<td>(Ignore) X</td>
<td>ignore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Not equal) DEFAULT</td>
<td>(Ignore) X</td>
<td>ignore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Not equal) DEFAULT</td>
<td>(Ignore) X</td>
<td>ignore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Not equal) DEFAULT</td>
<td>(Ignore) X</td>
<td>ignore</td>
</tr>
</tbody>
</table>
```

**Config Store AUTH_PROFILE_USER**
The template values describe that no user is allowed to be assigned to the authorization profile SAP_ALL. (The entry for user SAPSYS is a dummy entry.)
No change required

```
Target System : SEC_00 / Store Name : AUTH_PROFILE_USER

<table>
<thead>
<tr>
<th>PROFILES</th>
<th>USER</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SAP_ALL</td>
<td>USER IS AUTHORIZED</td>
</tr>
<tr>
<td></td>
<td>SAP_ALL</td>
<td>USER IS AUTHORIZED</td>
</tr>
</tbody>
</table>
```
Config Store SICF_SERVICES
The template values describe a set of SICF services should be deactivated according to several Security Notes.
No change required

Target System: SEC_00 / Store Name: SICF_SERVICES

Config Store SAP_KERNEL
The conditions describe which kernel release(s) or kernel patch levels are required.
Currently you cannot enter release specific patch levels, therefore it has limited use in a large mixed landscape containing systems on various releases.
Usually you would update the definition but for this workshop we keep the default values.

Config Store MS_SECINFO
The template values describe that no generic entry should be part of the access control file SECINFO of the message server.
Usually you would update the definition but for this workshop we keep the default values.
04 Maintain Target System for Configuration Validation

**Config Store GW_REGINFO**
The template values describe that no generic entry should be part of the access control file REGINFO of the gateway.
Usually you would update the definition but for this workshop we keep the default values.

**Config Store GW_SECINFO**
The template values describe that no generic entry should be part of the access control file SECINFO of the gateway.
Usually you would update the definition but for this workshop we keep the default values.

**Config Store GLOBAL**
The template values describe that the system should not be in modifiable state.
No change required
Config Store ABAP_NOTES
The template values describe which (security) notes should be applied to a system if required. You can update the definition, e.g. monthly to get the latest list of Security Notes which are checked by the EarlyWatch Alert / RSECNOTE as well.

To update the definition you

1. Select all entries
2. Delete the selected entries
3. Generate new entries based on the Online Recommendations for the EarlyWatch Alert / RSECNOTE
4. Save the data

(Instead of 1.-2. you can use the function “Delete non-selected entries” as well.)
Config Store ABAP_INSTANCE_PAHI

The template values describe the target values for profile parameters. The definition here should represent your Corporate Security Policy, therefore you should change some values.

Various operators are available to define conditions, see legend.
Example for a Regular Expression condition for the profile parameter login/ticket_expiration_time which accepts any time interval less than 12 hours as being compliant:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Operator</th>
<th>Value low</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/ticket_expiration_time</td>
<td>Regex</td>
<td>^1[0-1][1]:{0,1}[0-9][0-2]</td>
</tr>
</tbody>
</table>

Explanation:

```
^                     # the beginning of the string
1                     # '1'
[0-1]{1}               # any character of: '0' to '1' (1 times)
:{{0,1}}               # ':' (between 0 and 1 times (matching the most amount possible))
[0-9]{{0,2}}           # any character of: '0' to '9' (between 0 and 2 times (matching the most amount possible))
|                      # OR
^                     # the beginning of the string
0{{0,1}}              # '0' (between 0 and 1 times (matching the most amount possible))
[0-9]                 # any character of: '0' to '9'
:{{0,1}}              # ':' (between 0 and 1 times (matching the most amount possible))
[0-9]{{0,2}}          # any character of: '0' to '9' (between 0 and 2 times (matching the most amount possible))
```
05 Create Comparison System List for Configuration Validation

During this exercise we check the settings of critical system parameters using the Configuration Validation application within the SAP Solution Manager. The third step is to define the list of SAP systems which should be validated using a Target System.

Navigate to the tab “Comparison List Maintenance.”
Choose function “Create.”

1. Enter a Comparison List Name. Choose a unique name and enter a description.
2. Choose function “Display all” to view systems
3. Select ABAP systems
4. Choose function “Create from selected”

You get a confirmation message. Close the window.
06 Show Configuration Validation Report

During this exercise we check the settings of critical system parameters using the Configuration Validation application within the SAP Solution Manager. The last step is to produce the validation report.

Navigate to the tab “Report Execution”
1. Choose function “Display” to view references systems (target systems)
2. Select your Target System
3. Choose function “Display” to view Comparison Lists
4. Select your Comparison Lists
5. Scroll down (or close the section “Reference system and comparison systems”)

Ensure that you are working with “operator validation” reports. Choose a report to view non-compliant configuration items. Finally start the operator validation reporting.
On the next selection screen you can set additional filters for:

- Comparison systems (you have got the list from the Comparison List)
- Config store (e.g. ABAP_INSTANCE_PAHI)
- Configuration item (e.g. profile parameter)

However you can filter anything later on as well. Therefore we do not change the selection now.

Result:

Selected ConfigStores and Items - Only Non compliant Items with Value and Target Value
You can work with filters either using the navigation block of using the right-click sub menu on any value.

You can remove unnecessary drilldown columns.

You can swap columns, e.g. to produce a cross-system view per profile parameter.

(If you run into trouble while modifying filters or columns simply restart the report.)
Try to produce this view with following columns:
- Config. Item
- SAP System ID
- Config. Item Value
- Value of Target System
- Compliant (yes/no)

```
<table>
<thead>
<tr>
<th>Config. Item</th>
<th>SAP System ID</th>
<th>Config. Item Value</th>
<th>Value of Target System</th>
<th>Compliant (yes, no, ( \neq ) not valiated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth/check/caltransaction</td>
<td>M14</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/disable_multi_gui_login</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/disable_password_login</td>
<td>M14</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_diff</td>
<td>M14</td>
<td>1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_digits</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_ing</td>
<td>M14</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>login/min_password_specially</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/no_automatic_user_sapstar</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/password_expiration_time</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>login/ticket_only_by_https</td>
<td>M14</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>rdisp/accept_remote_tracce_level</td>
<td>M14</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>rdosp/gui_auto_logout</td>
<td>M14</td>
<td>8000</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>rdosp/gui_auto_logout</td>
<td>M38</td>
<td>8000</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>rdosp/gui_auto_logout</td>
<td>M38</td>
<td>8000</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```
07 Show Configuration Validation Report for Security Notes

During this exercise we check the settings of critical system parameters using the Configuration Validation application within the SAP Solution Manager.

Within Configuration Validation there exist a predefined report to validate the systems for missing but required security notes.

Navigate to the tab “Report Execution” and choose the section “Report Directory”

1. The report 0SECNOTE “Validation of SAP Notes using online recommendations” would run a similar analysis like the EarlyWatch Alert check on Security Notes / report RSECNOTE. This report checks for selected Security Notes!
   
   An automatic Target System 0GNRT001 will be created containing the Config Store ABAP_NOTES with values from the Online Recommendations for the EarlyWatch Alert about Security Notes.

2. Select the Comparison List SECURITY

3. Start the report
Result

You can rearrange and remove columns as usual. Any new view can be stored, too.
1. The report **SysRec_Security** “System Recommendations for Security Notes” shows the results of the application System Recommendations. This application checks for all Security Notes!

2. You have to select a (dummy) Reference System

3. You can select Comparison Systems. However, if you omit a selection, you get the result for all systems which have data

4. Finally, you start the report
Result:

**System Recommendations - SAP Notes**

<table>
<thead>
<tr>
<th>Selection: Reference and Comparison System, Config Store and Item(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty Demarcation, Empty Demarcation, Security, Empty Demarcation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>M10</td>
</tr>
<tr>
<td>M31</td>
</tr>
<tr>
<td>M37</td>
</tr>
<tr>
<td>M50</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notes - Systems according System Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>0000338119</td>
</tr>
<tr>
<td>0000490241</td>
</tr>
<tr>
<td>0000412309</td>
</tr>
<tr>
<td>0000512595</td>
</tr>
<tr>
<td>0000517484</td>
</tr>
<tr>
<td>0000526833</td>
</tr>
<tr>
<td>0000533496</td>
</tr>
<tr>
<td>000059383</td>
</tr>
<tr>
<td>0000598074</td>
</tr>
<tr>
<td>0000602194</td>
</tr>
</tbody>
</table>

Details

- Query View Selection
- Save View: ![Icon]
- Navigation Block:

**Configuration Items**

<table>
<thead>
<tr>
<th>System</th>
<th>Note</th>
<th>Version</th>
<th>Short Text</th>
<th>Component</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>M10 0000166119</td>
<td>0007 Restricting DB access to specific hosts</td>
<td>BC-DB-ORA</td>
<td>6 - Recom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000400241</td>
<td>0054 Problems with oppS or sap3 connect to Oracle</td>
<td>BC-DB-ORA</td>
<td>6 - Recom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000412309</td>
<td>0019 Authorization profile RFC user for IPCL</td>
<td>CRM-IPC</td>
<td>6 - Recom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000512595</td>
<td>0005 Report on potential SAP Virus</td>
<td>BC-SEC</td>
<td>1 - HotNl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000526833</td>
<td>0005 Buffer overflow in SAP ITS</td>
<td>BC-FES-ITS</td>
<td>1 - HotNl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000533496</td>
<td>0005 Composite SAP Note: SAP Web Dispatch</td>
<td>BC-CST-IC</td>
<td>6 - Recom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 000059383</td>
<td>0005 Security, Atage configuration files can be read</td>
<td>BC-FES-ITS</td>
<td>2 - Corre</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000602194</td>
<td>0004 No fullpath leakage to end-user</td>
<td>BC-FES-ITS</td>
<td>3 - Corre</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000602194</td>
<td>0004 SAP FSCN - Biller Direct: Stopping PUT requests</td>
<td>FIN-FSCN-BD-FE</td>
<td>2 - Corre</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M10 0000618516</td>
<td>0005 Security-related enhancement of RFCEEXEC program</td>
<td>BC-MID-RFC</td>
<td>2 - Corre</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Row: 1/1362