**3GPP TSG-SA3 Meeting #114e *ad-hoc draft\_S3-240045\_r1***

Electronic meeting, online, 22 - 26 January 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0160** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Updates threat references to TS 33.117 - clauses 4.3.4 to 4.3.5 |
|  |  |
| ***Source to WG:*** | ZTE Corporation |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph3 |  | ***Date:*** | 2024-01-15 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Updates threat references with clause numbers and threat names to TS 33.117. The existing threat references only point to TR 33.926 which is too general. Propose to add suitable threat reference examples for the security requirements and test cases. |
|  |  |
| ***Summary of change:*** | Updates of threat references in TS 33.117. |
|  |  |
| ***Consequences if not approved:*** | Incomplete Specification. |
|  |  |
| ***Clauses affected:*** | 4.3.4.2, 4.3.4.3, 4.3.4.4, 4.3.4.5, 4.3.4.6, 4.3.4.7, 4.3.4.8, 4.3.4.9, 4.3.4.10, 4.3.4.11, 4.3.4.12, 4.3.4.13, 4.3.4.14, 4.3.5.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Changes \*\*\*\*\*\*\*\*\*\*\*\*\*

#### 4.3.4.2 No system privileges for web server

*Requirement Name*: No system privileges for web server.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.

*Threat References*: TR 33.926 [4], clause 5.3.8, Elevation of privilege

*Test Case*:

***Test Name*:** TC\_NO\_SYSTEM\_PRIVILEGES\_WEB\_SERVER

**Purpose:**

Verify that the Web server is not run under system privileges.

**Procedure and execution steps:**

**Pre-Conditions:**

- The tester has needed administrative privileges.

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured /script adapted in line with the Requirement Description.

**Execution Steps**

1. Check that no web server processes runs with system privileges. Check that this is the case even for processes that may have been started by a user with system privileges.

a. Start the web server process as web server user and check process privileges.

b. If possible, start the web server process as with system privileges and check if process privileges get dropped.

2. Check in relevant system settings and web server configurations that a web server user is configured with minimal privileges needed to run the web server and the web server is executable by that user.

**Expected Results:**

- There are no findings of web server processes that run with system privileges.

- System settings have been found correctly set to ensure that no processes will run with system privileges.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files / command line output and screen shots of test executions

- Part of web server and/or system configuration (plain text or screenshot) showing the configured user for the web server process

- Test result (Passed or not)

#### 4.3.4.3 No unused HTTP methods

*Requirement Name*: No unused HTTP methods

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

HTTP methods that are not required shall be deactivated. Standard requests to web servers use GET, HEAD, and POST. If other methods are required, e.g, PUT, DELETE, PATCH, they shall not introduce security leaks such as TRACK or TRACE.

*Threat References*: TR 33.926 [4] clause 5.3.6.11, Unnecessary Services

*Test Case*:

***Test Name*:** TC\_NO\_UNUSED\_HTTP\_METHODS

**Purpose:**

Verify that the Web server has deactivated all HTTP methods that are not required.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has needed administrative privileges.

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

- Check that relevant system settings and configurations are correct to ensure fulfilment of the requirement.

**Expected Results:**

- System settings and configurations have been found adequately set, in all Web components of the system, to ensure that unneeded HTTP methods are deactivated.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions

- Test result (Passed or not)

#### 4.3.4.4 No unused add-ons

*Requirement Name*: No unused add-ons

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

*Threat References*: TR 33.926 [4], clause 5.3.6.11, Unnecessary Services

*Test Case*:

***Test Name*:** TC\_NO\_UNUSED\_ADD-ONS

**Purpose:**

To verify that the Web server has deactivated unneeded add-ons and unneeded scripting components.

**Procedure and execution steps**

**Pre-Conditions:**

- The vendor has supplied a list of add-ons or scripting tools for Web server components needed for system operation, and that therefore need to be exempted from the test investigation.

- The tester has administrative privileges.

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

1. Check that the web server is only running and listening on known ports (e.g. tcp port 80 and/or 443). Check that CGI or other scripting components, Server Side Includes (SSI), and WebDAV are deactivated if they are not required. See also guidance under 4.3.4.12.

2. Check that nothing else has been installed than the web server.

3. Check that relevant system settings and configurations are correct to ensure fulfilment of the requirement.

**Expected Results:**

- System settings and configurations have been found adequately set, in all Web components of the system, to ensure that all unneeded add-ons or script components are deactivated.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions.

- Test result (Passed or not).

#### 4.3.4.5 No compiler, interpreter, or shell via CGI or other server-side scripting

*Requirement Name*: No compiler, interpreter, or shell via CGI or other server-side scripting.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory - or other corresponding scripting directory - shall not include compilers or interpreters (e.g. PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).

*Threat Reference*: TR 33.926 [4]

*Test Case*:

***Test Name*:** TC\_NO\_COMPILER\_FOR\_CGI

**Purpose:**

To verify that there are no compilers, interpreters or shell accessible via CGI or other scripting components.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has administrative privileges

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured /script adapted in line with the Requirement Description.

**Execution Steps**

1. Consult the web server configuration to identify all directories used for CGI or other scripting components.

2. Check that there are no compilers or interpreters (e.g., PERL® interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells) in the directory/directories used for CGI or for other scripting tools (including PERL®, PHP, and others).

**Expected Results:**

There are no compilers, interpreters or shells in directories accessible via CGI or other scripting components.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions.

- Part of web server configuration (plaintext or screenshot) showing all directories accessible by the CGI/scripting components.

- List of files (with types and permissions, if available) inside the directories accessible by the CGI/scripting components.

- Test result (Passed or not).

#### 4.3.4.6 No CGI or other scripting for uploads

*Requirement Name*: No CGI or other scripting for uploads.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

*Threat References*: TR 33.926 [4], clause 5.3.8.3, Folder Write Permission Abuse

*Test Case*:

**Test Name:** TC\_NO\_CGI\_OR\_SCRIPTING\_FOR\_UPLOADS

**Purpose:**

To test whether the upload directory is equal to the CGI/Scripting directory.

**Procedure and execution steps:**

**Pre-Condition:**

If the web server is configured with CGI/Scripting on, this test applies.

**Execution Steps**

**Execute the following steps:**

The tester checks whether the upload directory is configured to be different from the CGI/Scripting directory.

**Expected Results:**

The configured upload directory is different from the CGI/Scripting directory.

Additional evidence might be provided that shows that the web server has no write rights for the CGI/Scripting directory.

**Expected format of evidence:**

A part of the configuration file / screenshot of the configuration showing that the web server is properly configured.

#### 4.3.4.7 No execution of system commands with SSI

*Requirement Name*: No execution of system commands with SSI.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

*Threat Reference*: TR 33.926 [4], clause 5.3.8, Elevation of privilege

*Test Case*:

**Test Name**: TC\_NO\_EXECUTION\_OF\_SYSTEM\_COMMANDS

**Purpose:**

To test whether it is possible to use the exec directive and if so, whether it can be used for system commands.

**Procedure and execution steps:**

**Pre-Condition:**

If the web server is configured with SSI active, this test applies.

**Execution Steps**

**Execute the following steps:**

1.-The tester checks whether execution of system commands is disabled in the web server configuration.

2. The tester actually attempts to use the exec directive in an SSI file with and without system commands.

**Expected Results:**

- The execution of system commands via SSIs exec directive is disabled in the web server configuration.

- It is impossible to execute system commands via SSIs exec directive.

**Expected format of evidence:**

- A part of the configuration file / screenshot of the configuration showing that the web server is properly configured. For example, a configuration file that shows that the IncludesNOEXEC (Apache HTTP Server®) or ssiExecDisable (Microsoft® IIS) is set.

- Web server log while executing step 2.

#### 4.3.4.8 Access rights for web server configuration

*Requirement Name*: Access rights for web server configuration files

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.

*Threat References*: TR 33.926 [4], clause 5.3.8, Elevation of privilege

*Test Case*:

***Test Name*:** TC\_ACCESS\_RIGHTS\_WEB\_SERVER\_FILES

**Purpose:**

To verify that the access rights for Web server configuration files are correctly set.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has administrative privileges

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

- Check the access rights settings for Web server system configuration files.

- Check that relevant system settings and configurations are correct to ensure fulfilment of the requirement.

**Expected Results:**

- Access rights for system configuration files are adequately set.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions

- Test result (Passed or not)

#### 4.3.4.9 No default content

*Requirement Name*: No default content.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.

*Threat References*: TR 33.926 [4], clause 5.3.6.8, Insecure Default Configuration

*Test Case*:

***Test Name*:** TC\_NO\_DEFAULT\_CONTENT

**Purpose:**

To verify that there is no default content on the web server, that is not needed for web server operation, since such default content can be useful for an attacker.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has needed administrative privileges

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

1. Check that all default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server has been removed.

**Expected Results:**

- No default content (examples, help files, documentation, aliases, un-needed directories or manuals) has been found to remain on any Web server component.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions.

- Test result (Passed or not).

#### 4.3.4.10 No directory listings

*Requirement Name*: No directory listings / Directory Browsing.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: Directory listings (indexing) / "Directory browsing" shall be deactivated.

*Threat References*: TR 33.926 [4], clause 5.3.6.9, File/Directory Read Permissions Misuse

*Test Case*:

***Test Name*:** TC\_NO\_DIRECTORY\_LISTINGS

**Purpose:**

To verify that Directory listings / Directory browsing has been deactivated in all Web server components.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has administrative privileges

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

- Check that Directory listings (indexing) / "Directory browsing" has been deactivated in all Web server components.

**Expected Results:**

- Evidence that Directory listing / Directory browsing has been deactivated in all Web server components.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions

- Test result (Passed or not)

#### 4.3.4.11 Web server information in HTTP headers

*Requirement Name*: Web server information in HTTP headers.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: The HTTP header shall not include information on the version of the web server and the modules/add-ons used.

*Threat References*: TR 33.926 [4], clause 5.3.6.5, System Fingerprinting

*Test Case*:

***Test Name*:** TC\_NO\_WEB\_SERVER\_HEADER\_INFORMATION

**Purpose:**

To verify that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has administrative privileges

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

1. Check that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

**Expected Results:**

- Evidence that HTTP headers do not include information on the version of the web server and the modules/add-ons used.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions

- Test result (Passed or not)

#### 4.3.4.12 Web server information in error pages

*Requirement Name*: Web server information in error pages.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the web server shall be replaced by error pages defined by the vendor.

*Threat References*: TR 33.926 [4], 5.3.6.5, System Fingerprinting

*Test Case*:

***Test Name*:** TC\_NO\_WEB\_SERVER\_ERROR\_PAGES\_INFORMATION

**Purpose:**

To verify that error pages and error messages do not include information about the web server.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has needed administrative privileges.

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

- Check that generated error pages and error messages do not include information about the web server.

**Expected Results:**

- Evidence that generated error pages and error messages do not include information about the web server.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions

- Test result (Passed or not)

#### 4.3.4.13 Minimized file type mappings

*Requirement Name*: Minimized file type mappings *Requirement Reference*: In accordance with industry best practice

*Requirement Description*: File type- or script-mappings that are not required shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

*Threat References*: TR 33.926 [4], clause 5.3.6.13, Unnecessary Applications

*Test Case*:

***Test Name*:** TC\_NO\_WEB\_SERVER\_FILE\_TYPE MAPPINGS

**Purpose:**

To verify that file type- or script-mappings that are not required have been deleted.

**Procedure and execution steps**

**Pre-Conditions:**

- The tester has needed administrative privileges.

- A tester machine is available.

- Recommended: an automatic assessment tool has been configured / script adapted in line with the Requirement Description.

**Execution Steps**

- Check that all file type- or script-mappings that are not required have been deleted.

**Expected Results:**

- Evidence that all file type- or script-mappings, that are not required, have been deleted.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Log files and screen shots of test executions

- Test result (Passed or not)

#### 4.3.4.14 Restricted file access

*Requirement Name*: Restricted file access.

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*: Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the web server's document directory. In particular, the web server shall not be able to access files which are not meant to be delivered.

*Threat References*: TR 33.926 [4], clause 5.3.6.9, File/Directory Read Permissions Misuse

*Test Case*:

**Test Name:** TC\_RESTRICTED\_FILE\_ACCESS

**Purpose:**

To test whether the restrictive access rights are assigned to all files which are directly or indirectly in the web server's document directory and to verify whether path traversal is made improbable.

**Procedure and execution steps:**

**Pre-Condition:**

1. The web server is configured according to the manual

**Execution Steps**

**Execute the following steps:**

1. The tester verifies that access rights on the servable content (meaning directories and files) is set to the following:

a. The files are owned by the user that runs the web server;

b. The files are not writable to others, except the web server's account;

2. The tester verifies that the user running the web server is an unprivileged account;

3. For Operating Systems that have chrooted environments, the tester verifies that the web server runs inside a jail or chrooted environment.

**Expected Results:**

 - Name of user running the web server with the privileges of the account;

 - Access rights of files and directories that the web server serves;

 - Configuration that shows that the web server is in a chrooted environment.

**Expected format of evidence:**

A part of the configuration file / screenshot of the configuration showing that the web server, the file access rights and the account running the web server is properly configured.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Changes \*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Changes \*\*\*\*\*\*\*\*\*\*\*\*\*

### 4.3.5 Network Devices

#### 4.3.5.1 Traffic Separation

*Requirement Name*: Traffic Separation

*Requirement Reference*: In accordance with industry best practice

*Requirement Description*:

The network product shall support physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 [3] for further information.

*Threat References*: TR 33.926 [4], clause 5.3.6.15, lack of GNP traffic isolation

*Test case*:

**Test Name:** TC\_TRAFFIC\_SEPARATION

**Purpose:**

To test whether traffic belonging to different network domains is separated.

**Procedure and execution steps:**

**Pre-Condition:**

NOTE: This test applies if the network product is meant to handle traffic from different network domains, e.g. both O&M and control plane traffic.

The network product has at least two separate (logical) interfaces dedicated to different network domains. Network products for which the test applies and that fail to meet this precondition fail the test by definition.

**Execution Steps**

**Execute the following steps:**

1. The tester checks whether the network product refuses traffic intended for one network domain on all interfaces meant for the other network domain, and vice versa.

2. Step 1 is to be performed for all pairs of different network domains.

**Expected Results:**

The two tests are successful.

**Expected format of evidence:**

A PASS or FAIL.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Changes \*\*\*\*\*\*\*\*\*\*\*\*\*