**3GPP TSG-SA3 Meeting #114e ad-hoc *S3-240107***

**Electronic meeting, online, 22 - 26 January 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Handling of IP options and extensions | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | \_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 can be 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:*** | | This test case refers to IP packets with "unnecessary options", but do not define what is meant by "unnecessary options". Define what is meant by “unnecessary options”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is suggested to reference RFC 7126. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear text specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 4.2.4.1.1.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] Void

[3] IETF RFC 3871: "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] Void

[6] Void

[7] Void

[8] Void

[9] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[10] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[11] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[12] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[13] 3GPP TS 29.501: "Principles and Guidelines for Services Definition".

[14] Void

[15] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[16] IETF RFC 7515:"JSON Web Signature (JWS)".

[17] IETF RFC 7519:"JSON Web Token (JWT)".

[18] 3GPP TS 23.501: "System Architecture for the 5G System".

[19] 3GPP TR 33.916: "Security Assurance Methodology (SECAM) for 3GPP network products".

[x] IETF RFC 7126: "Recommendations on Filtering of IPv4 Packets Containing IPv4 Options".

\*\*\* 2nd CHANGE \*\*\*

4.2.4.1.1.3 Handling of IP options and extensions

*Requirement Name*: Handling of IP options and extensions

*Requirement Reference:* In accordance with industry best practice

*Requirement Description*:

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

*Threat References*: TR 33.926 [4]

*Test Case*:

The test for this requirement can be carried out using a suitable tool or manually by performing the steps described below. If a tool is used then the tester needs to provide evidence, e.g. by referring to the documentation of the tool, that the tool actually provides functionality equivalent to the steps described below.

**Test Name**: TC\_HANDLING-IP-OPTIONS-AND-EXTENSIONS

**Purpose:** To verify that the network product provides functionality to filter out IP packets with unnecessary options or extension headers in reference to RFC 7126 [x].

**Procedure and execution steps:**

**Pre-Conditions:**

- The vendor declares in the documentation accompanying the network product at least the following information:

- The support of filtering capability for IP packets with unnecessary options or extensions headers.

- The actions performed by the network product when an IP packet with unnecessary options or extensions headers is received (e.g. the packet is dropped, the options or extensions are ignored and the packet is treated as if it has no IP options, etc.) .

- Guidelines on how to enable and configure this filtering capability.

- The network product has at least one physical interface named if1 supporting both IPv4 and IPv6. If the network product does not support IPv6 then IPv6 related steps and checks are skipped**.**

- A network traffic analyser on the network product (e.g. TCPDUMP) or an external traffic analyser directly connected to the network product is available .

- The tester has administrative privileges.

- A tester machine is available with a tool able to send IPv4 packets with the IP Options and IPv6 packets (if supported by the network product) with Extension Header set (e.g. Scapy).

**Execution Steps**

1. The tester logs in the network product.

2. The tester configures on the network product a filtering rule to drop all IP packets containing an IP Option set

a) The tester establishes an O&M session on if1 interface

b) Using the tool (e.g. Scapy) the tester sends from the tester machine an IPv4 TCP SYN packet with an appropriate destination portto if1 interface without setting any IP Options

c) Using the network traffic analyser, the tester verifies that the IP packet is received by the network product and the tester verifies that the corresponding ACK message is sent back.

d) Using the tool (e.g. Scapy) the tester sends an IPv4 TCP SYN packet with an appropriate destination port and an IP Option set to the if1 interface

e) Using the network traffic analyser, the tester verifies that the IP packet is received by the network product but no ACK message is sent back. This confirms the packet is dropped as expected from the filtering rule.

3. The tester configures on the network product a filtering rule to drop all incoming packets based on specific Extension Header Types, e.g. packets with the Routing Header extension. Skip Step 3 if the network product does not support IPv6.

a) Using the tool (e.g. Scapy) the tester sends from the tester machine an IPv6 TCP SYN packet with an appropriate destination port to if1 interface without setting any extension header

b) Using the network traffic analyser, the tester verifies that the IP packet is received by the network product and the tester verifies that the corresponding ACK message is sent back.

c) Using the tool (e.g. Scapy) the tester sends an IPv6 TCP SYN packet with an appropriate destination port and an extension header set to the if1 interface

d) Using the network traffic analyser, the tester verifies that the IP packet is received by the network product but no ACK message is sent back. This confirms the packet is dropped as expected from the filtering rule.

**Expected Results:**

The network product discards IPv4 packets with unnecessary options in reference to RFC 7126 [x] or IPv6 packets (assuming the network product supports IPv6) with extension header.

**Expected format of evidence:**

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

- Used tools and their configurations

- Settings and configurations used

- Pcap trace

- Screenshot

- Test result (Passed or not)

\*\*\* END OF CHANGES \*\*\*