IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution for CIDs 3017 3023 3016 |
| Date: December 16, 2022 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Abhishek Patil | Qualcomm Inc. |  |  | appatil@qti.qualcomm.com |
| Alfred Asterjadhi |  |  |  |
| Duncan Ho |  |  |  |
| George Cherian |  |  |  |
| Gaurang Naik |  |  |  |
| Yanjun Sun |  |  |  |
| Abdel Karim |  |  |  |

 Abstract

This submission proposes resolutions for the following CIDs received against REVme D2.0 during LB270: 3017 3023 3016

Revisions:

* Rev 0: Initial version of the document.

***TGm editor: Please note baseline for this document is REVme D2.0***

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGm Draft. This introduction is not part of the adopted material.

***Editing instructions formatted like this are intended to be copied into the TGm Draft (i.e., they are instructions to the 802.11 editor on how to merge the text with the baseline documents).***

***TGm Editor: Editing instructions preceded by “TGm Editor” are instructions to the TGm editor to modify existing material in the TGm draft. As a result of adopting the changes, the TGm editor will execute the instructions rather than copy them to the TGm Draft.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Pg/Ln** | **Section** | **Comment** | **Proposed Change** | **Resolution** |
| 3017 | Abhishek Patil | 1967.18 | 10.25.7 | In addition to the conditions specified in the paragraph starting P1967L18, the scoreboard context at the recipient STA must not be updated if MPDU decryption or integrity check fails. This can happen when an attacker injects a fake Data frame in such case, the decryption will fail. | The commenter will provide a contribution to address this. | **Revised**Agree with the comment. The *injection of a fake* *frame* attack will go undetected until the decryption step of the frame processing. However, by then, the sequence control will have an incorrect entry. As a result, a genuine Data frames that is subsequently received will be dropped if the rogue frame has moved the window such that SN of the genuine frame falls outside the current window or the SN of the rogue frame is the same as that of the subsequent genuine frame (i.e., duplicate detection).The resolution proposes that the recipient STA flushes the scoreboard context after each TXOP (i.e., maintain partial state) when the negotiated block ack agreement is a protected block ack agreement. With this, any updates to *WinStartR* (by a fake frame) will be forgotten so that reception of subsequent (genuine) frame is not affected. Furthermore, it recommends that the originator solicit immediate blockack for frames transmitted during the TXOP by the end of the TXOP so that the receive status for those frames is not lost.**TGm editor, please make changes as shown in 11-22/2212r0 tagged 3017** |
| 3023 | Abhishek Patil | 2838.61 | 12.5.2.3.3 | With bits 4-15 masked, the Sequence Number field is unprotected which opens the door for several attack scenarios (such as replaying a Data frame with modified SN or injecting a fake Data frame. | The SN should be protected (i.e., not mask the bits), at least when block ACK agreement is a protected BA. | **Revised**Agree with the comment. Unprotected Sequence Number field enables an attacker to replay previously transmitted Data frame(s) with modified SN(s). Such attack goes undetected until the PN-based replay check is performed. However, this is too late since by then the sequence control and the reorder buffer will be updated. As a result, a genuine Data frames that is subsequently received will be dropped if the preceding rogue frame has moved the SN such that SN of the genuine frame falls outside the current window or is the same. Protected Sequence Number field (by not masking the field during AAD construction) will help detect such attacks much sooner and not update the *WinStartB*. The proposed resolution requires Sequence Number to be protected when the negotiated block ack agreement is a protected block ack agreement.**TGm editor, please make changes as shown in 11-22/2212r0 tagged 3023** |
| 3016 | Abhishek Patil | 1967.18 | 10.25.7 | In addition to the conditions specified in the paragraph starting P1967L18, the scoreboard context and the reorder buffer at the recipient STA must not be updated if an MPDU fails replay check. This can happen when an attacker replays a valid MPDU with an updated SN. Such MPDU will pass decryption but will fail replay check. | The commenter will provide a contribution to address this. | **Revised**Agree with the comment. The *replayed MPDU with modified SN* attack is possible since the Sequence Number field in the MAC header is not protected. Such attack will go undetected until PN-based replay check is performed. However, this is too late in the sequence of frame processing. By then, the *WinStartB* & *WinStartR* will be updated, and the sequence control and reorder buffer, each, will have an incorrect entry. As a result, a genuine Data frames that is subsequently received will be dropped if the rogue frame has moved the window such that SN of the genuine frame falls outside the current window or the SN of the rogue frame is the same as that of the subsequent genuine frame (i.e., duplicate detection).The resolution proposes two changes: 1. Protecting the Sequence Number field (by not masking it during AAD construction) when the negotiated block ack agreement is a protected block ack agreement. With this change, a frame carrying a tampered SN will not pass the decryption block and thus prevent reorder buffer from getting updated due to a rogue frame. See resolution for CID 3023.
2. Require that the recipient maintains partial state when the negotiated block ack agreement is a protected block ack agreement. This way the scoreboard context is flushed after each TXOP. Any updates to the *WinStartR* (by the replayed frame) will be forgotten so that reception of subsequent frame is not affected based on the SN of a previous frame. Furthermore, it is recommended that the originator solicit immediate blockack for frames transmitted during the TXOP by the end of the TXOP so that the receive status for those frames is not lost. See resolution for CID 3017

**TGm editor, please make changes as shown in 11-22/2212r0 tagged 3017 and 3023** |

* **Protected block ack agreement**[3017]

***TGm editor: Please add a new bullet to the 4th paragraph this subclause as shown below:***

A STA that has successfully negotiated a protected block ack agreement shall obey the following rules for that agreement as a block ack recipient in addition to rules specified from 10.25.6.3 (Scoreboard context control during full-state operation) to 10.25.6.6 (Receive reordering buffer control operation):

* The STA shall implement partial-state operation and discard the temporary record after the end of the current TXOP.

***TGm editor: Please add a new bullet to the 3rd paragraph this subclause as shown below:***

A STA that has successfully negotiated a protected block ack agreement shall obey the following rule as a block ack originator in addition to rules specified in 10.25.6.7 (Originator’s behavior) and 10.25.6.8 (Maintaining block ack state at the originator):

* The originating STA should solicit an immediate BlockAck frame for the MPDU that are transmitted during a TXOP by the end of the TXOP (e.g., via an MPDU with Ack Policy set to Implicit BAR or by sending a PBAC WinStart Update frame).

NOTE – If the originator is unable to solicit an immediate BlockAck frame for MPDUs transmitted during a TXOP by the end of that TXOP, then the received status of those MPDU is lost.

**12.5.2.3.3 Construct AAD**[3023]

***TGm editor: Please update the 5th bullet under item a) in this subclause as shown below:***

1. SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked out if the negotiated block ack agreement is not a protected block ack agreement and with the Sequence Number subfield unmodified if the negotiated block ack agreement is a protected block ack agreement. The Fragment Number subfield is not modified.