**WGQ EDM and RMQ IR/TEIS Work Paper**

05/21/20

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sandia Issue1** | **Sandia Report2** | **Issue Summary** | **NAESB Response** | **WGQ Standards created/modified in response to this issue** | **RMQ Standards created/modified in response to this issue** |
| 13 | BusOps | Consider options to mitigate replay and amplification attacks | TBD |  |  |
| 5 | Add | Whitelisting | TBD |  |  |
|  |  | Refnum | TBD |  |  |

1 Not all identified issues were relevant to WGQ/RMQ, so the issue numbering contains gaps.

2 BusOps = Business Operations Practices and Standards Report; Add = Addendum Report

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 13. | Business Operations Practices and Standards Report – Section 6.1.6 Continued Use of Different Security Paradigms (Pages 13 – 15)  (Table of Contents Section 6.2.3 Gas and Electric Industry Interactions) | Finally, IET business process as currently implemented may be vulnerable to both replay[[1]](#footnote-1) and amplification[[2]](#footnote-2) attacks. Based on the assessment teams review of the transactional process these two attacks were immediately identified as attacks of concern…  Note that this attack is feasible even with payloads that are encrypted with foreign, untrusted keys, or with payloads that are filled with garbage bits. Two basic approaches exist to help eliminate this kind of amplification attack. The first strategy involves making error notification messages to be as small as possible and smaller than the original requests. This way, an attacker using this mechanism will not be able to amplify the volume of data sent to a target; rather, as the response message is smaller, the overall denial-of-service risk will be correspondingly lowered. The second strategy uses rate limiting to ensure that error messages are sent at a rate that is lower than expected message processing speeds. This way, even if the responses are larger than the adversary-submitted requests, they will not be sent to the target at a rate that would strain target computational resources. | The subcommittees should consider standard(s) to address mitigation of replay and amplification attacks as aligned with recommended strategies | Jointly between WGQ EDM and RMQ IR/TEIS  WEQ Cybersecurity Subcommittee | 07/22/2020 Homework: Ask IT about the capability of monitoring and flagging excessive error rate tagging. Also, see if there is any data to help define a limit. |
| 5. | Addendum Report Section 2.3.2 – Ukrainian Power Grid Attack (Pages 23 – 25) | A relatively static communications environment, such as the NAESB-responsible systems, should definitely be considered for whitelisting. However, how whitelisting is implemented will be a hardware-specific implementation and thus outside NAESB standards scope. In consideration of the whitelisting ROI are several factors:   * Some related information must be made publicly available and this must not be blocked by the whitelisting implementation. * Since NAESB standards do not specify the environment there could be negative impacts to non-EDI applications which are hosted on the same servers.   The whitelisting decision must consider the support environment. The point being that if a legitimate transaction is blocked by the whitelisting, how quickly could the error be corrected given coverage and capability of the support team? | Subcommittees should consider standard(s) to incorporate whitelisting as a best practice which should be followed | Jointly between WGQ EDM and RMQ IR/TEIS | FAQ of Appendix B in IET Manual:  **Q11: Does NAESB require whitelisting?**  A: NAESB Internet ET participants are encouraged to use whitelisting in EDI/EDM and FF/EDM transactions. Whitelisting should not be considered for Customer Activities or Information Postings web sites. |
|  | Refnum  Refnum\_Orig  **Section 6.1.2 – NAESB Standards Need Review for Unused or Unnecessary Functionality** | As part of an annual review the analysis team recommends review of NIST 800-52 for guidance. Monitoring of required protocols as defined in WEQ-002.3 and the IET data dictionary tableupdates for acceptable configurations for supported secure communication protocols defined for IET are all recommended for immediate update as required by independent facility implementation based on NIST NVD, US CERT, ICS CERT or vendor mandate. The assessment team recommends any updates for these communication protocols to be considered for incorporation into standards following review as an updated minimum version as included in the Wholesale Gas Electronic Delivery Mechanism Related Standards and incorporated by FERC in 18 CFR 284.12, updating to the latest versions of available protocols as soon as practicable and not to exceed 9 months is a general best practice that organizations within the wholesale electric quadrant, retail electric and retail gas quadrants should consider for incorporation as well. | As electronic communication standards evolve at a rapid rate, functionality that was necessary to ensure accurate communications can become unnecessary. The assessment team did not identify any vulnerabilities in the standards they reviewed but did identify optional fields in the WGQ/REQ/Internet Electronic Transport Related Standards that could prove to be an attack vector in the future. The fields that are identified by the IET data dictionary as mutually agreed (not mandatory) are time-c qualifier, and refnum, refnum-orig, and transaction-set. As part of the annual review the assessment team recommends a survey review for these data fields that may no longer be utilized to determine if they data fields can be removed. Unused data fields can be leveraged to cause undefined system states that can lead to unwanted system behavior. |  | As part of the annual review the assessment team recommends a survey review for these data fields that may no longer be utilized to determine if they data fields can be removed. and Standard Nos. 10.1.10 and 4.3.104. |

1. *Replay Attacks*, retrieved on June 10, 2019, from <https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks> [↑](#footnote-ref-1)
2. *DNS Amplification Attacks*, retrieved on June 10, 2019, from <https://www.us-cert.gov/ncas/alerts/TA13-088A> [↑](#footnote-ref-2)