CFRG at IETF 121

Errata Overview: November 2024

Nick Sullivan

Overview of the Errata Process for IRTF

Submission and Vetting

- Errata for IRTF documents are submitted online.
- The IRTF Chair or relevant Working Group Chairs initially vet the submissions.
- The vetting process determines if the errata correct errors or introduce substantive changes.

Approval and Recording

- Approved errata are recorded in the RFC Editor's errata system.
- This recording ensures that corrections or clarifications are part of the document's official record.
- The process informs future readers about any updates to the document.

RFC 7748: Elliptic Curves for Security

Errata 7096

- Recommendation: Hold
- Details: Tooling code change for test vectors.

Errata 7824

- Recommendation: Verify
- Details: Involves updates to the test vectors provided in the RFC.
- Priority: High
- **Action Required:** Verification by authors and investigation of implementations to see if they are affected.

Errata 7879

- Recommendation: Rejected
- Confirmation: Rejection confirmed by Watson Ladd on the mailing list.

RFC 8032: Edwards-Curve Digital Signature Algorithm (EdDSA)

Errata 5968

- **Recommendation**: Verify
- Security Impact: Likely low
- Issue: Boundary equality definitions are excluded from a value that is derived from a hash
- Concern: Is there code that fails on 0 or -1?
- **Action Required:** Verification by authors.

Errata 6306, 6348, 7031

- **Recommendation**: Hold for document update
- Issues: Notation and editorial issues on attribution/reference.

RFC 8391: eXtended Merkle Signature Scheme

Errata 6352

- **Recommendation**: Hold
- **Priority:** Medium
- **Nature:** Editorial
- **Issue:** Involves a non-trivial change in reference format.

Errata 6821

- **Recommendation**: Verify
- **Priority:** High
- **Nature:** Conflict
- **Issue:** Length in bytes vs max integer value conflict.
- **Action Required:** Verification by authors and investigation of implementations to see if they are affected.

Errata 7420

Recommendation: Verify

- **Priority:** Medium
- **Nature:** Undefined
- **Issue:** setXMSS_SK is undefined
- **Action Required:** Guidance needed from implementers if this has been an issue.

RFC 8439: ChaCha20 and Poly1305 for IETF Protocols

Errata 6569

- **Recommendation**: Hold
- Issue: Incorrect endianness in description.
- Concern: Potential exploitability if misinterpreted

Errata 6989

- **Recommendation**: Verify
- Priority: Medium
- Issue: Missing nibble
- **Action**: Verification needed

Errata 7880

- **Recommendation**: Verify
- Priority: Medium
- Issue: Off-by-one error
- Concern: Implementations should be checked
- **Action**: Verification needed

RFC 8554: Leighton-Micali Hash-Based Signatures

Errata 7409

- **Recommendation**: Verify
- **Priority:** Medium
- **Issue**: Incorrect sizes in the signature table.
- **Confirmed by:** Scott Flurer
- **Action Required:** Verification submission

Errata 7994

- **Recommendation**: Hold
- **Issue**: Variable name consistency with external documents

RFC 9180: Hybrid Public Key Encryption

Errata 7121

- **Recommendation**: Verify
- **Priority**: Medium
- **Details**: Unclamped test vectors for RFC 7748 curves
- **Action**: Verification needed

Errata 7251, 7933, 7934

- **Recommendation**: Hold
- **Priority**: Medium
- **Details**: Several (not security critical) clarifications recommended.
- **Action**: Confirmation from authors

Errata 7937

- **Recommendation**: Verify
- **Priority**: Medium
- **Details**: Missing required parameters for underlying functions.
- **Action**: Verification needed