Javascript Object Signing and Encryption
Internet-Draft
Updates: 7518 (if approved)
Intended status: Standards Track
Expires: 4 October 2025

N. Madden
Teya

2 April 2025

JOSE: Deprecate 'none' and 'RSA1_5'
draft-ietf-jose-deprecate-none-rsa15-02

Abstract

This document updates [RFC7518] to deprecate the JWS algorithm "none" and the JWE algorithm "RSA1_5". These algorithms have known security weaknesses. It also updates the Review Instructions for Designated Experts to establish baseline security requirements that future algorithm registrations should meet.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://NeilMadden.github.io/jose-deprecate-none-rsa1_5/draft-ietf-jose-deprecate-none-rsa15.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-jose-deprecate-none-rsa15/.

Discussion of this document takes place on the Javascript Object Signing and Encryption Working Group mailing list (mailto:jose@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/jose/. Subscribe at https://www.ietf.org/mailman/listinfo/jose/.

Source for this draft and an issue tracker can be found at https://github.com/NeilMadden/jose-deprecate-none-rsa1_5.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

JSON Web Algorithms (JWA, [RFC7518]) introduced several standard algorithms for both JSON Web Signature (JWS) and JSON Web Encryption (JWE). Many of these algorithms have stood the test of time and are still in widespread use. However, some algorithms have proved to be difficult to implement correctly leading to exploitable vulnerabilities. This document deprecates two such algorithms:

* The JWS "none" algorithm, which indicates that no security is applied to the message at all.

* The JWE "RSA1_5" algorithm, which indicates RSA encryption with PKCS#1 version 1.5 padding.

Note that RSA signatures using PKCS#1 version 1.5 padding (RS256, RS384, and RS512) are unchanged by this specification and can still be used.

Additionally, this document also updates the Review Instructions for the JOSE Designated Experts, to establish baseline security requirements for future JOSE algorithm registrations. Only algorithms that are reasonably believed to satisfy these requirements should be registered in future.

1.1. The 'none' algorithm

The "none" algorithm creates an Unsecured JWS, whose contents are completely unsecured as the name implies. Despite strong guidance in the original RFC around not accepting Unsecured JWS by default, many implementations have had serious bugs due to accepting this algorithm. In some cases, this has led to a complete loss of security as authenticity and integrity checking can be disabled by an adversary simply by changing the algorithm ("alg") header in the JWS. The website [howmanydays] tracks public vulnerabilities due to implementations mistakenly accepting the "none" algorithm. It currently lists 12 reports, many of which have high impact ratings. The following is a partial list of issues known to have been caused by misuse of the "none" algorithm, with a Common Vulnerability Enumeration [CVE] identifier, and a Common Vulnerability Scoring System [CVSS] score indicating the severity of the impact:

* CVE-2018-1000531 (https://nvd.nist.gov/vuln/detail/CVE-2018-1000531) - CVSS: 7.5 (High)

* CVE-2017-10862 (https://nvd.nist.gov/vuln/detail/CVE-2017-10862) - CVSS: 5.3 (Medium)

* CVE-2022-23540 (https://nvd.nist.gov/vuln/detail/CVE-2022-23540) - CVSS: 7.6 (High)

* CVE-2020-15957 (https://nvd.nist.gov/vuln/detail/CVE-2020-15957) - CVSS: 7.5 (High)

* CVE-2021-29500 (https://nvd.nist.gov/vuln/detail/CVE-2021-29500) - CVSS: 7.5 (High)

* CVE-2021-29451 (https://nvd.nist.gov/vuln/detail/CVE-2021-29451) - CVSS: 9.1 (Critical)

* CVE-2021-29455 (https://nvd.nist.gov/vuln/detail/CVE-2021-29455) - CVSS: 7.5 (High)

* CVE-2021-22160 (https://nvd.nist.gov/vuln/detail/CVE-2021-22160) - CVSS: 9.8 (Critical)

* CVE-2021-32631 (https://nvd.nist.gov/vuln/detail/CVE-2021-32631) - CVSS: 6.5 (Medium)

* CVE-2023-29357 (https://nvd.nist.gov/vuln/detail/CVE-2023-29357) - CVSS: 9.8 (Critical)

Many other vulnerabilities have been reported without an accompanying CVE, which we do not list here.

Although there are some legitimate use-cases for Unsecured JWS, these are relatively few in number and can easily be satisfied by alternative means. The small risk of breaking some of these use-cases is far outweighed by the improvement in security for the majority of JWS users who may be impacted by accidental acceptance of the "none" algorithm.

1.2. The ’RSA1_5’ algorithm

The "RSA1_5" algorithm implements RSA encryption using PKCS#1 version 1.5 padding [RFC8017] (section 7.2). This padding mode has long been known to have security issues, since at least Bleichenbacher’s attack in 1998. It was supported in JWE due to the wide deployment of this algorithm, especially in legacy hardware. However, more secure replacements such as OAEP [RFC8017] or elliptic curve encryption algorithms are now widely available. NIST has disallowed the use of this encryption mode for federal use since the end of 2023 [NIST.SP800-131Ar2] and a CFRG draft [I-D.irtf-cfrg-rsa-guidance] also deprecates this encryption mode for IETF protocols. This document therefore also deprecates this algorithm for JWE.

1.3. Guidance on deprecation

Both of the algorithms listed above are deprecated for use in JOSE—the none algorithm for JWS, and RSA1_5 for JWE. JOSE library developers should deprecate support for these algorithms. Application developers MUST disable support for these algorithms by default. New specifications building on top of JOSE MUST NOT allow the use of either algorithm.

The IANA algorithm registry distinguishes between algorithms that are "Deprecated" and those that are "Prohibited". The algorithms identified in this document are to be marked as Deprecated only. Existing specifications and applictions that make use of these algorithms can continue to do so, but should consider adopting alternatives in future updates.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Security Considerations

This entire document is concerned with security, since the security of JOSE implementations directly affects the security of systems that include them (see for example the long list of CVEs in Sec. 1.1).

4. IANA Considerations

4.1. JOSE Algorithm Deprecations

The following changes are to be made to the IANA JOSE Web Signature and Encryption Algorithms registry:

* For the entry with Algorithm Name "none", update the JOSE Implementation Requirements to "Deprecated".

* For the entry with Algorithm Name "RSA1_5", update the JOSE Implementation Requirements to "Deprecated".

4.2. Updated Review Instructions for Designated Experts

The review instructions for the designated experts for the IANA "JSON Web Signature and Encryption Algorithms" registry [IANA.jose] in Section 7.1 of [RFC7518] are updated to add these additional review criteria:

* For JWS signature algorithms, only algorithms that are reasonably conjectured to meet the standard security goal of existential unforgeability under a chosen message attack (EUF-CMA) should be considered for approval. See textbooks such as [BonehShoup] (section 13.1.1) for a definition of existential unforgeability.

* For JWE key management algorithms (specified with the "alg" header), only algorithms that are reasonably conjectured to meet the standard security goal of indistinguishability under an adaptive chosen ciphertext attack (IND-CCA2) should be considered for approval, as defined in textbooks such as [BonehShoup] (section 9.2.2 and chapter 12).

* For JWE content encryption methods (specified with the "enc" header), only algorithms that are reasonably conjectured to meet the standard security goal of authenticated encryption with associated data (AEAD) should be considered for approval. See [RFC5116] and textbooks, such as [BonehShoup] (section 9.1), for the definition of AEAD security.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <https://www.rfc-editor.org/rfc/rfc5116>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/rfc/rfc7518>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

5.2. Informative References

[BonehShoup] Boneh, D. and V. Shoup, "A Graduate Course in Applied Cryptography (v0.6)", 14 January 2023, <https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_6.pdf>.

[CVE] MITRE, "Common Vulnerability Enumeration Database", n.d., <https://cve.mitre.org>.

[CVSS] FIRST, "Common Vulnerability Scoring System", n.d., <https://www.first.org/cvss/>.

[howmanydays]
Sanderson, J., "How Many Days Has It Been Since a JWT alg:none Vulnerability?", 25 September 2023, <https://github.com/zofrex/howmanydayssinceajwtalgnonevuln/blob/deploy/data/vulns.yml>.

[I-D.irtf-cfrg-rsa-guidance]
Kario, A., "Implementation Guidance for the PKCS #1 RSA Cryptography Specification", Work in Progress, Internet-Draft, draft-irtf-cfrg-rsa-guidance-03, 20 February 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-rsa-guidance-03>.

[IANA.jose]
IANA, "JSON Object Signing and Encryption (JOSE)", <https://www.iana.org/assignments/jose>.

[NIST.SP800-131Ar2]
Barker, E. and A. Roginsky, "Transitioning the use of cryptographic algorithms and key lengths", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-131ar2, March 2019, <https://doi.org/10.6028/nist.sp.800-131ar2>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/rfc/rfc8017>.

Appendix A. Acknowledgments

The author would like to thank the following people for feedback and useful suggestions: Mike Ounsworth, Michael Jones, Yaron Sheffer, and John Mattsson.

Author's Address

Neil Madden
Teya
Email: neil.e.madden@gmail.com