TABLE OF CONTENTS

Third Party Security Advisories

DRAFT FOR REVIEW

07/25/2022 06:35:06

This document will list briefings on each third party security issue found and give a description, a timeline on updating component, an acknowledgment that the solution is included in tagged release.

TLDR;

CVE	Exposure	Recommended Stable Tags
CVE-2021-3449 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2021-3450 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2021-3711 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2021-3712 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2021-4160 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2022-0778 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2022-1292 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2022-2068 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205
CVE-2022-2097 - OpenSSL	No cryptopkg Exposure	1.1.1j, edk2-stable202105 1.1.1n, edk2-stable202205

Process

(short form)

1. Security Bugs reported through: National Vulnerability Database
2. The issue is evaluated for EDK2 exposure
3. Determine Timeline for updating to Master
4. Update third party component list updated in version tag

Revision History

Revision	Revision History	Date
.001.0	Initial release. Logs 1 - 9	Jul 20, 2022

1. CVE-2021-3449 - OPENSSL

Published: 03/25/2021

Recommendation:

Edk2 TLS supports client mode only. This issue only exists in server mode.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

2. CVE-2021-3450 - OPENSSL

Published: 03/25/2021

Recommendation:

X509_V_FLAG_X509_STRICT is never set by edk2.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

3. CVE-2021-3711 - OPENSSL

Published: 08/24/2021

Recommendation:

The SM2 algorithm is not supported by EDK2.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

4. CVE-2021-3712 - OPENSSL

Published: 08/24/2021

Recommendation:

Analysis has confirmed that the relevant OpenSSL string operations have been used correctly and safely in EDK2.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

5. CVE-2021-4160 - OPENSSL

Published: 01/28/2022

Recommendation:

The issue only affects MIPS platforms, and we don’t have MIPS in EDK2.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

6. CVE-2022-0778 - OPENSSL

Published: 03/15/2022

Recommendation:

EDK2 does not use the BN_mod_sqrt() function.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

7. CVE-2022-1292 - OPENSSL

Published: 05/03/2022

Recommendation:

EDK2 never calls the c_rehash.in script in normal build process.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

8. CVE-2022-2068 - OPENSSL

Published: 06/21/2022

Recommendation:

EDK2 never calls the c_rehash.in script in normal build process.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag

9. CVE-2022-2097 - OPENSSL

Published: 07/05/2022

Recommendation:

EDK2 does not enable AES OCB mode or use the 32-bit AES-NI assembly optimizations.

Until further notice, the following versions of OpenSSL are appropriate to use within the EDK2 CryptoPkg:

- OpenSSL 1.1.1j, updated in the edk2-stable202105 stable tag
- OpenSSL 1.1.1n, updated in the edk2-stable202205 stable tag