November 3, 2023

Overall rating: Medium

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of an OpenSSL vulnerability. A vulnerability has been identified in the processing of key and initialisation vector (IV) lengths. This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers. The vulnerability affects OpenSSL versions 3.0 and 3.1.

Technical Details

When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed afterthe key and IV have been established. Any alterations to the key length, via the "keylen" parameter or the IV length, via the "ivlen" parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB.

For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse.

Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical.

Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore, it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However, if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **MEDIUM** risk. A software update exists to address this risk. OpenSSL 3.0 users should upgrade to OpenSSL 3.0.12. OpenSSL 3.1 users should upgrade to OpenSSL 3.1.4

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-5363
- OpenSSL Security Advisory
- VRM Vulnerability Reports