🏠 » Tech Updates / Security Advisories » Buffer overread in DTLS ClientHello parsing

Buffer overread in DTLS ClientHello parsing

Title	**Buffer overread in DTLS ClientHello parsing.**
CVE	CVE-2022-35409
Date	2022-07-11
Affects	All versions of Mbed TLS up to and including 2.28.0 and 3.1.0
Impact	A remote attacker may cause a crash or information disclosure
Severity	Medium
Credit	Cybeats PSI Team

Vulnerability

An unauthenticated remote host can send an invalid ClientHello message in which the declared length of the cookie extends past the end of the message. A DTLS server with `MBEDTLS_SSL_DTLS_CLIENT_PORT_REUSE` enabled will read past the end of the message up to the declared length of the cookie.

At this point in the parsing, the message is stored in a buffer with room for `MBEDTLS_SSL_IN_CONTENT_LEN` bytes plus headers. The data beyond the end of the message has been wiped, so there is no risk of information disclosure from the buffer. Therefore this is a vulnerability only if the purported length of the cookie extends beyond the end of the buffer.

Since the length of the cookie is limited to 255 bytes, the vulnerability is only present if `MBEDTLS_SSL_IN_CONTENT_LEN` is small. The threshold depends on the exact configuration. The default value of `MBEDTLS_SSL_IN_CONTENT_LEN` is large enough to avoid the vulnerability.

The default cookie check function `mbedtls_ssl_cookie_check()` does not read the cookie if its length is not the expected length (28 bytes if SHA-256 is enabled).

Impact

An unauthenticated remote host can cause a buffer overread of up to 255 bytes on the heap in vulnerable DTLS servers. This may lead to a crash or to information disclosure via the cookie check function.

Resolution

Affected users will want to upgrade to Mbed TLS 3.2.0 or 2.28.1 depending on the branch they're currently using.

Work-around

A sufficiently large value of `MBEDTLS_SSL_IN_CONTENT_LEN` avoids the vulnerability. The threshold depends on the exact configuration. For example:

- With default options regarding DTLS and only support for AEAD ciphersuites, and using the default cookie check function `mbedtls_ssl_cookie_check()`, the threshold is 210 bytes.
- With `MBEDTLS_SSL_DTLS_CONNECTION_ID` enabled, the threshold can be up to 258 bytes if using `mbedtls_ssl_cookie_check()`.
- In the worst case, with a custom cookie check function, the threshold can be up to 571 bytes.

Turning off `MBEDTLS_SSL_DTLS_CLIENT_PORT_REUSE` also avoids the vulnerability.