April 19, 2024

Overall rating: High

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. The vulnerability affects OpenSSL versions prior to 3.2.2, 3.1.6, 3.0.14 and 1.1.1y. Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions.

Technical Details

An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service

This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured, and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state, and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation.

This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients.

Of note the FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

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

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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-2024-2511
- Tenable CVE-2024-2511
- OpenSSL
- VRM Vulnerability Reports