February 9, 2024

Overall rating: Medium

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 OpenSSL 3.2.1, OpenSSL 3.1.5, OpenSSL 3.0.13, OpenSSL 1.1.1x and OpenSSL 1.0.2zj.

Technical Details

A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue.

Note: All OpenSSL versions before 1.1.1 are out of support and no longer receiving updates. Extended support is available for 1.0.2 from OpenSSL Software Services for premium support customers.

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

This vulnerability is rated as a **MEDIUM** 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-2024-0727
- OpenSSL
- VRM Vulnerability Reports