**Title**: Out-of-date Version (OpenSSL)

**Scope**: http://zero.webappsecurity.com/

**Details**: Netsparker identified you are using an out-of-date version of OpenSSL.

**Severity**: Critical

**Date**: 2021-07-31 18:49:21

**By**: **Rahul Vashistha** (rahulvashistha1412@gmail.com)

**Vulnerability Details:**

**Identified Version:** 0.9.8e (contains 5 critical and 107 other vulnerabilities)

**Latest Version:** 1.1.1k

**Impact:**

Since this is an old version of the software, it may be vulnerable to attacks.

**Remedy:**

Please upgrade your installation of OpenSSL to the latest stable version.

**Classification:**

PCI v3.1-6.2; PCI v3.2-6.2; CAPEC-310; CWE-937, 1035; HIPAA-164.308(a)(1)(i); ISO27001-A.14.1.2; OWASP PC-C1; OWASP 2013-A9; OWASP 2017-A9

**Helpful Use Case:**

[OpenSSL Heartbleed Vulnerability: Risks and Remediation](https://www.netsparker.com/server-security-software/openssl-heartbleed-vulnerability-scanner/)

**Known Vulnerabilities in this Version:**

1. **Medium**: OpenSSL Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

The dtls1\_buffer\_record function in ssl/d1\_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of "future epoch" DTLS records that are buffered in a queue, aka "DTLS record buffer limitation bug."

1. **Critical:** OpenSSL Numeric Errors Vulnerability

Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary code via unspecified vectors.

1. **Critical:** OpenSSL Improper Input Validation Vulnerability

OpenSSL before 0.9.8m does not check for a NULL return value from bn\_wexpand function calls in (1) crypto/bn/bn\_div.c, (2) crypto/bn/bn\_gf2m.c, (3) crypto/ec/ec2\_smpl.c, and (4) engines/e\_ubsec.c, which has unspecified impact and context-dependent attack vectors.