Severe Vulnerability in OpenSSL

2nd April 2022

Ticket Number: EN250308

This advisory is sent out in part that stakeholders hold preventative management and precautions of their network.

Summary

A high severity vulnerability has been disclosed in OpenSSL. CVE-2022-0778, which has a CVSS score of 7.5-, is an infinite loop vulnerability in OpenSSL when parsing invalid certificates. Exploitation of this vulnerability can lead to a Denial of Service (DoS) attack on the application. The vulnerability affects OpenSSL versions:

- 1.0.2
- 1.1.1
- 3.0

CSIRTMalta encourages everyone to update the affected versions to the latest versions where this vulnerability has been patched, i.e., versions 1.0.2zd, 1.1.n and 3.0.2.

Additional Information and References:

1. CVE-2022-0778
2. Impact of the OpenSSL Infinite Loop Vulnerability

CSIRTMalta Team

MINISTRY FOR HOME AFFAIRS
NATIONAL SECURITY AND LAW ENFORCEMENT