Advisory Alert

Alert Number: AAA20240116 **Date:** January 16, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
OpenSSL	Low	Denial of Service Vulnerability

Description

Affected Product	**OpenSSL**
Severity	Low
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-6237)
Description	OpenSSL has released a security update addressing a denial-of-service vulnerability in applications that use the EVP_PKEY_public_check() function to check RSA public keys. When an RSA key that contains an overly large prime number obtained from an untrusted source is checked using the function EVP_PKEY_public_check(), it would take a long time to process. It is recommended by OpenSSL to apply necessary security fixes at earliest to avoid issues
.Affected Products	OpenSSL versions 3.0.0 to 3.0.12 OpenSSL versions 3.1.0 to 3.1.4 OpenSSL versions 3.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20240115.txt

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.