Advisory Alert

Alert Number: AAA20220316 **Date:** March 16, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
OpenSSL	**High**	Denial-Of-Service (Dos) Vulnerability
Apache	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**OpenSSL**
Severity	**High**
Affected Vulnerability	Denial-Of-Service (Dos) Vulnerability (CVE-2022-0778)
Description	OpenSSL released updates to address a high-severity denial-of-service (DoS) vulnerability, that affects the BN_mod_sqrt() function used when certificate parsing. An attacker can trigger the vulnerability by crafting a malformed certificate with invalid explicit curve parameters.
Affected Products	OpenSSL
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20220315.txt

Affected Product	**Apache**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22719, CVE-2022-22720, CVE-2022-22721, CVE-2022-23943)
Description	The Apache Software Foundation released a security update to address multiple vulnerabilities in the HTTP Server and its modules. A remote attacker could exploit the vulnerabilities by sending a specially crafted request to the affected systems. • CVE-2022-22719 - mod_lua Use of uninitialized value of in r:parsebody • CVE-2022-22720 - HTTP request smuggling vulnerability • CVE-2022-22721 - Possible buffer overflow with very large or unlimited LimitXMLRequestBody • CVE-2022-23943 - Out-of-bounds Write vulnerability in mod_sed
Affected Products	Apache HTTP Server 2.4.52 and earlier. Apache HTTP Server 2.4 version 2.4.52 and prior versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.