Advisory Alert

Alert Number : AAA20211231 **Date :** December 31, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache	**High**	**Multiple Vulnerabilities**

Description

Affected Product	**Apache**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Apache has released security patch update addressing vulnerabilities that exist in their products **CVE-2021-44224 -** A crafted URI sent to httpd configured as a forward proxy can cause a crash or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint. **CVE-2021-44790 –** Vulnerability that exits in apache HTTP server leads to cause a buffer overflow in the mod_lua multipart parser by sending a carefully crafted request body
Affected Products	Apache HTTP Server 2.4.7 up to 2.4.51 Apache HTTP Server 2.4.51 and earlier
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.