Advisory Alert

Alert Number: AAA20211011 **Date:** October 11, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache	**Critical**	Multiple Vulnerabilities

Description

Affected Product	Apache
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-42013)
Description	The vulnerability exists in Apache HTTP server due to an insufficient fix for the path traversal vulnerability (CVE-2021-41733). A remote attacker could exploit this vulnerability by sending specially crafted request to map URLs to files outside the directories configured by Alias like directives. Successful exploitation of this vulnerability could allow the attacker to execute arbitrary code, if CGI scripts are also enabled for these aliased paths and may result in complete compromise of vulnerable system. These vulnerabilities have been exploited in the wild, Users are highly recommended to update to the latest version 2.4.51 to mitigate the risk associated with the flaw.
Affected Products	Apache 2.4.50, 2.4.49
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-42013

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.