Advisory Alert

Alert Number: AAA20211006 **Date:** October 6, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	Apache
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-41524, CVE-2021-41773)
Description	Apache has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-41524 – Null pointer dereference vulnerability was detected during HTTP/2 request processing which could allow an external source to perform DoS attack by sending a specially crafted request. CVE-2021-41773 - Vulnerability was discovered in a change made to path normalization in Apache HTTP Server 2.4.49 which could lead an attacker to use a path traversal attack to map URLs to files outside the expected document root. This request can succeed if files outside of the document root are not protected by "require all denied" and this flaw could leak the source of interpreted files like CGI scripts. **This issue is known to be exploited in the world and affects only Apache 2.4.49.** It is highly recommended by Apache to apply necessary security fixes at earliest to avoid issues.
Affected Products	Apache HTTP Server 2.4.49
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Affected Product	Fortinet
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-24019, CVE-2020-15941, CVE-2021-36175, CVE-2021-26105, CVE-2021-36178, CVE-2021-24021, CVE-2021-36170)
Description	Fortinet has released security updates addressing multiple vulnerabilities that exists in their products including information disclosure, unauthorized code execution, buffer over flaw and privilege escalation. Fortinet highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiClientEMS version 6.4.2 and below. FortiClientEMS version 6.4.1 and below. FortiClientEMS version 6.2.8 and below. FortiWebManager version 6.2.3 and below. FortiWebManager version 6.0.x. FortiSandbox 4.0.0. FortiSandbox 3.2.2 and below. FortiSandbox 3.1.4 and below. FortiSDNConnector version 1.1.7 or below FortiAnalyzer version 6.4.3 and below. FortiAnalyzer version 6.2.7 and below. FortiAnalyzer version 6.0.x.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-20-072 https://www.fortiguard.com/psirt/FG-IR-20-074 https://www.fortiguard.com/psirt/FG-IR-20-027 https://www.fortiguard.com/psirt/FG-IR-20-234 https://www.fortiguard.com/psirt/FG-IR-20-183 https://www.fortiguard.com/psirt/FG-IR-20-098 https://www.fortiguard.com/psirt/FG-IR-21-112

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.