Advisory Alert

Alert Number: AAA20211215 **Date:** December 15, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	**Multiple Vulnerabilities**
Apache	**Medium**	**Denial of Service Vulnerability**

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-40452, CVE-2021-40453, CVE-2021-41360, CVE-2021-41365, CVE-2021-42293, CVE-2021-42294, CVE-2021-42295, CVE-2021-42309, CVE-2021-42310, CVE-2021-42311, CVE-2021-42312, CVE-2021-42313, CVE-2021-42314, CVE-2021-42315, CVE-2021-42320, CVE-2021-43214, CVE-2021-43215, CVE-2021-43216, CVE-2021-43217, CVE-2021-43222, CVE-2021-43224, CVE-2021-43227, CVE-2021-43235, CVE-2021-43236, CVE-2021-43243, CVE-2021-43244, CVE-2021-43255, CVE-2021-43256, CVE-2021-43875, CVE-2021-43880, CVE-2021-43882, CVE-2021-43888, CVE-2021-43889, CVE-2021-43899, CVE-2021-43905)
Description	Microsoft has released Security Updates addressing multiple vulnerabilities that exists with multiple Microsoft products, features and roles. In addition to security changes for the vulnerabilities, updates include defense-in-depth updates to help improve security-related features. It is highly recommended by Microsoft to apply necessary security fixes at earliest to avoid issues.
Affected Products	Windows Media Microsoft Windows Codecs Library Microsoft Defender for IoT Internet Storage Name Service Microsoft Local Security Authority Server (lsasrv) Windows Encrypting File System (EFS) Windows DirectX Microsoft Message Queuing Windows Remote Access Connection Manager Windows Storage Spaces Controller Windows SymCrypt Windows NTFS Windows Event Tracing Remote Desktop Client Role: Windows Fax Service Windows Storage Windows Update Stack Windows Kernel Windows Digital TV Tuner Role: Windows Hyper-V Windows Common Log File System Driver Azure Bot Framework SDK Windows TCP/IP Office Developer Platform Microsoft Office ASP.NET Core & Visual Studio Visual Studio Code Microsoft Devices Windows Print Spooler Components Windows Mobile Device Management Windows Installer Microsoft PowerShell
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Dec

Affected Product	**Apache**
Severity	**Medium**
Affected Vulnerability	Denial of service vulnerability (CVE-2021-45046)
Description	Apache has released Security Updates addressing denial of service vulnerability that exists in their products. It was discovered by Apache that the provided fix addressing CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could lead attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 restricts JNDI LDAP lookups to localhost by default. And the previous mitigations involving configuration such as setting the system property log4j2.noFormatMsgLookup to true do NOT mitigate this specific vulnerability. Apache highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	all versions from 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://logging.apache.org/log4j/2.x/security.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.