



# Advisory Alert

Alert Number: AAA20220923

Date: September 23, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

## Overview

Product	Severity	Vulnerability
Microsoft	Low	Spoofing Vulnerability

## Description

Affected Product	Microsoft
Severity	Low
Affected Vulnerability	Spoofing Vulnerability (CVE-2022-37972)
Description	Microsoft has released a security update addressing the spoofing vulnerability that exists in Microsoft Endpoint Configuration Manager. An attacker could exploit this vulnerability to obtain sensitive information. Microsoft recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Microsoft Endpoint Configuration Manager versions 2103-2207
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37972">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37972</a>

## 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.