



# Advisory Alert

Alert Number: AAA20241224

Date: December 24, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

## Overview

Product	Severity	Vulnerability
Dell	High	Code Execution Vulnerability

## Description

Affected Product	Dell
Severity	High
Affected Vulnerability	Code Execution Vulnerability (CVE-2024-52535)
Description	<p>Dell has released security updates addressing a Local Code Execution Vulnerability that exists in their products.</p> <p><b>CVE-2024-52535</b> - Dell SupportAssist for Home PCs versions 4.6.1 and prior and Dell SupportAssist for Business PCs versions 4.5.0 and prior, contain a symbolic link (symlink) attack vulnerability in the software remediation component. A low-privileged authenticated user could potentially exploit this vulnerability, gaining privileges escalation, leading to arbitrary deletion of files and folders from the system.</p> <p>Dell advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	SupportAssist for Home PCs Versions prior to 4.6.2 SupportAssist for Business PCs Versions prior to 4.5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.dell.com/support/kbdoc/en-us/000261086/dsa-2024-470-security-update-for-dell-supportassist-for-home-pcs-and-dell-supportassist-for-business-pcs-vulnerabilities">https://www.dell.com/support/kbdoc/en-us/000261086/dsa-2024-470-security-update-for-dell-supportassist-for-home-pcs-and-dell-supportassist-for-business-pcs-vulnerabilities</a>

## Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.