Advisory Alert

Alert Number: AAA20210506 **Date:** May 6, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	**Insufficient Access Control Vulnerability**
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	**Insufficient Access Control Vulnerability**
Severity	**Critical**
Affected Vulnerability	Dell (CVE-2021-21551)
Description	Dell dbutil_2_3.sys driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required. Dell highly recommends to apply necessary fixes to the product at earliest to avoid issues.
Affected Products	For Dell Platform Tags: 4.0.30.0, A04 or greater For Dell System Inventory Agent: 2.6.0.0 or greater
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/ro-ro/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-insufficient-access-control-vulnerability

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1490, CVE-2021-1438, CVE-2021-1507, CVE-2021-1486, CVE-2021-1478, CVE-2021-1532, CVE-2021-1447,CVE-2021-1234, CVE-2021-1535, CVE-2021-1514, CVE-2021-1513, CVE-2021-1509, CVE-2021-1510, CVE-2021-1512, CVE-2021-1284, CVE-2021-1515, CVE-2021-1275, CVE-2021-1468, CVE-2021-1400,CVE-2021-1401, CVE-2021-1520, CVE-2021-1421,CVE-2021-1521, CVE-2021-1363, CVE-2021-1365, CVE-2021-1397,CVE-2021-1499, CVE-2021-1497, CVE-2021-1498, CVE-2021-1516, CVE-2021-1530, CVE-2021-1519,CVE-2021-1426, CVE-2021-1427, CVE-2020-3347, CVE-2021-1493, CVE-2020-27122)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exists with multiple cisco products. It is highly recommended to apply necessary fixes provided on the official Cisco website at the earliest to avoid these security issues and all Cisco users are encouraged to upgrade latest versions
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&impact=critical,high,medium&last_published=2021%20May&sort=-last_published#~Vulnerabilities

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.