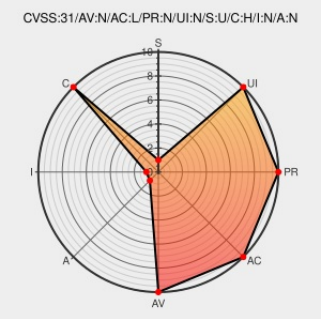
CVE-2023-4990

Published on: Not Yet Published

Last Modified on: 10/16/2023 07:14:00 PM UTC

CVE-2023-4990

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mcl-net from Mcl-collection contain the following vulnerability:

Directory traversal vulnerability in MCL-Net versions prior to 4.6 Update Package (P01) may allow attackers to read arbitrary files.

CVE-2023-4990 has been assigned by product-security@gg.jp.panasonic.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **MCL Technologies** - **MCL-Net** version **<= 4.6 Update Package (P01)**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
MCL Mobility Platform as-a-Service	www.mcl-mobilityplatform.com text/html	MISC www.mcl-mobilityplatform.com/downloads.php

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Mcl-collection	Mcl-net	-	All	All	All
Operating System	Mcl-collection	Mcl-net Firmware	All	All	All	All

cpe:2.3:h:mcl-collection:mcl-net:-:*:*:*:*:*:*:*:

cpe:2.3:o:mcl-collection:mcl-net_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→