



CVE-2022-36642

Published on: Not Yet Published

Last Modified on: 09/27/2022 03:40:00 PM UTC

CVE-2022-36642

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Omnia Mpx Node](#) from [Telosalliance](#) contain the following vulnerability:

A local file disclosure vulnerability in /appConfig/userDB.json of Telos Alliance Omnia MPX Node through 1.0.0-1.4.9 allows attackers to access users credentials which makes him able to gain initial access to the control panel with high privilege because the cleartext storage of sensitive information which can be unlatched by exploiting the LFD

vulnerability.

CVE-2022-36642 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
Omnia Node MPX Auth Bypass via LFD - Cyber Guy's Blog	cyber-guy.gitbook.io text/html	MISC cyber-guy.gitbook.io/cyber-guy/pocs/omnia-node-mpx-auth-bypass-via-lfd
Omnia MPX 1.5.0+r1 - Path Traversal - Hardware remote Exploit	www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/50996
Omnia MPX Node	www.telosalliance.com text/html	MISC www.telosalliance.com/radio-processing/audio-interfaces/omnia-mpx-node
Update your browser to use Google Drive, Docs, Sheets, Sites, Slides, and Forms - Google Drive Help	drive.google.com text/html	MISC drive.google.com/drive/folders/1jm9h8JNmezTt7AbHYRY7gPC4IXGDNkIL

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Telosalliance	Omnia Mpx Node	-	All	All	All
Operating System	Telosalliance	Omnia Mpx Node Firmware	All	All	All	All
Operating System	Telosalliance	Omnia Mpx Node Firmware	1.5.0	-	All	All
Operating System	Telosalliance	Omnia Mpx Node Firmware	1.5.0	r1	All	All
cpe:2.3:h:telosalliance:omnia_mpx_node:-:*:*:*:*:*:						
cpe:2.3:o:telosalliance:omnia_mpx_node_firmware:*:*:*:*:*:						
cpe:2.3:o:telosalliance:omnia_mpx_node_firmware:1.5.0:-:*:*:*:*:						
cpe:2.3:o:telosalliance:omnia_mpx_node_firmware:1.5.0:r1:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-36642 : A local file disclosure vulnerability in /appConfig/userDB.json of Telos Alliance Omnia MPX Node t... twitter.com/i/web/status/1...	2022-09-02 22:02:25
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-36642 A local file disclosure vulnerability in /appConfig/userDB.json o... twitter.com/i/web/status/1...	2022-09-02 23:56:00
 /r/netcve	CVE-2022-36642	2022-09-02 23:38:41

[← Previous ID](#)

[Next ID →](#)

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)