



CVE-2022-30621

Published on: Not Yet Published

Last Modified on: 07/22/2022 04:29:00 PM UTC

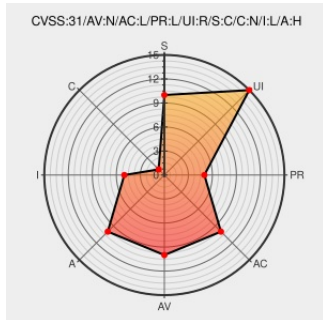
CVE-2022-30621

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Cellinx Nvt - Ip Ptz Camera](#) from [Cellinx](#) contain the following vulnerability:

Allows a remote user to read files on the camera's OS "GetFileContent.cgi". Reading arbitrary files on the camera's OS as root user.

CVE-2022-30621 has been assigned by [cna@cyber.gov.il](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cellinx](#) - **Cellinx NVT - IP PTZ Camera** version **>= 3.2.1**

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Attention Required! Cloudflare	web.archive.org text/html Inactive Link Not Archived	MISC www.gov.il/en/departments/faq/cve_advisories

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 	Cellinx	Cellinx Nvt - Ip Ptz Camera	-	All	All	All
Operating System	Cellinx	Cellinx Nvt - Ip Ptz Camera Firmware	3.2.0	All	All	All
Operating System	Cellinx	Cellinx Nvt - Ip Ptz Camera Firmware	3.2.1	All	All	All
cpe:2.3:h:cellinx:cellinx_nvt_-_ip_ptz_camera:-:*:*:*:*:*:						
cpe:2.3:o:cellinx:cellinx_nvt_-_ip_ptz_camera_firmware:3.2.0:*:*:*:*:*:						
cpe:2.3:o:cellinx:cellinx_nvt_-_ip_ptz_camera_firmware:3.2.1:*:*:*:*:*:						
Discovery Credit						
MetaData						
Social Mentions						
Source	Title					Posted (UTC)
 @CVEreport	CVE-2022-30621 : Allows a remote user to read files on the camera's OS "GetFileContent.cgi". Reading arbitrary file... twitter.com/i/web/status/1...					2022-07-18 13:06:06
 @threatmeter	CVE-2022-30621 Allows a remote user to read files on the camera's OS "GetFileContent.cgi". Reading arbitrary files... twitter.com/i/web/status/1...					2022-07-18 23:25:45
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-30621 - Allows a remote user to read files on the camera's OS "GetFileContent... twitter.com/i/web/status/1...					2022-07-18 23:25:56
 @threatmeter	CVE-2022-30621 Allows a remote user to read files on the camera's OS "GetFileContent.cgi". Reading arbitrary files... twitter.com/i/web/status/1...					2022-07-19 07:09:10
 /r/netcve	CVE-2022-30621					2022-07-18 14:38:58
← Previous ID			Next ID →			

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)