



# CVE-2021-32941

Published on: Not Yet Published

Last Modified on: 06/07/2022 02:51:00 PM UTC

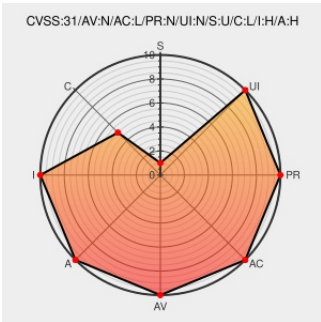
## CVE-2021-32941 - advisory for ICSA-21-238-02

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **N48pbb** from **Annke** contain the following vulnerability:

Annke N48PBB (Network Video Recorder) products of version 3.4.106 build 200422 and prior are vulnerable to a stack-based buffer overflow, which allows an unauthorized remote attacker to execute arbitrary code with the same privileges as the server user (root).

CVE-2021-32941 has been assigned by [ics-cert@hq.dhs.gov](mailto:ics-cert@hq.dhs.gov) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Annke](#) - **N48PBB (NVR)** version <= **V3.4.106 build 200422**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>COMPLETE</b>	<b>COMPLETE</b>	<b>COMPLETE</b>


## CVE References

Description	Tags	Link
Annke Network Video Recorder   CISA	<a href="http://www.cisa.gov">www.cisa.gov</a> <a href="#">text/html</a>	<a href="https://www.cisa.gov/uscert/ics/advisories/icsa-21-238-02">MISC www.cisa.gov/uscert/ics/advisories/icsa-21-238-02</a>

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](mailto: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 	<a href="#">Annke</a>	<a href="#">N48pbb</a>	-	All	All	All
Operating System	<a href="#">Annke</a>	<a href="#">N48pbb Firmware</a>	All	All	All	All
Operating System	<a href="#">Annke</a>	<a href="#">N48pbb Firmware</a>	3.4.106	-	All	All
Operating System	<a href="#">Annke</a>	<a href="#">N48pbb Firmware</a>	3.4.106	build_200422	All	All

cpe:2.3:h:annke:n48pbb:-:\*:\*:\*:\*:\*:

cpe:2.3:o:annke:n48pbb\_firmware:\*:\*:\*:\*:\*:








cpe:2.3:o:annke:n48pbb\_firmware:3.4.106:-:\*:\*:\*:\*:


cpe:2.3:o:annke:n48pbb\_firmware:3.4.106:build\_200422:\*:\*:\*:\*:

### Discovery Credit

Andrea Palanca from Nozomi Networks reported this vulnerability to CISA.

### Social Mentions

Source	Title	Posted (UTC)
 @InfosecurityMag	Nozomi Networks found remote code execution vulnerability CVE-2021-32941 in the web service of the Annke N48PBB net... <a href="#">twitter.com/i/web/status/1...</a>	2021-08-27 11:30:02
 @thehackbr	Novidades? Nenhuma: mais uma vulnerabilidade crítica (CVE-2021-32941) foi encontrada em um modelo de câmeras de seg... <a href="#">twitter.com/i/web/status/1...</a>	2021-08-27 19:30:18
 @ipssignatures	The vuln CVE-2021-32941 has a tweet created 0 days ago and retweeted 10 times. <a href="#">twitter.com/InfosecurityMa...</a> #pow1rtrtwcve	2021-08-28 01:06:00
 @twelvesec	Critical #IoT camera flaw (CVE-2021-32941) allows for device hijacking. #CyberSecurity, #infosec, #privacy... <a href="#">twitter.com/i/web/status/1...</a>	2021-08-29 04:12:04
 @InfosecurityMag	Nozomi Networks found remote code execution vulnerability CVE-2021-32941 in the web service of the Annke N48PBB net... <a href="#">twitter.com/i/web/status/1...</a>	2021-08-29 08:30:01
 @PCDUE	Nozomi Networks found remote code execution vulnerability CVE-2021-32941 in the web service of the Annke N48PBB net... <a href="#">twitter.com/i/web/status/1...</a>	2021-08-29 08:46:20
 @blackcellteam	? Nozomi Networks Labs has discovered a critical Remote Code Execution (RCE) vulnerability (CVE-2021-32941) relate... <a href="#">twitter.com/i/web/status/1...</a>	2021-09-08 10:51:25

 @EXN_NA	#Nozomi Labs has discovered a critical #RCE vulnerability (CVE-2021-32941) related to the web service of the #Annke... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-09-09 15:01:19
 @CVEreport	CVE-2021-32941 : Annke N48PBB Network Video Recorder products of version 3.4.106 build 200422 and prior are vulne... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-05-23 19:06:22
 @wvdsteen	New vulnerability on the NVD: CVE-2021-32941 <a href="https://ift.tt/qygeSis">ift.tt/qygeSis</a> May 24, 2022 at 07:16AM	2022-05-23 20:16:55
 /r/netcve	<a href="#">CVE-2021-32941</a>	2022-05-23 20:38:28

[← 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](https://status.cve.report)**