



CVE-2021-33045

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-33045
State	PUBLIC
Assigner	cybersecurity@dahuatech.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-15 22:15:00 UTC
Updated	2021-12-02 13:49:00 UTC
Description	The identity authentication bypass vulnerability found in some Dahua products during the login process. Attackers can bypa

Risk And Classification

EPSS: 0.941410000 probability, percentile 0.999130000 (date 2026-04-02)

CISA KEV: Listed on 2024-08-21; due 2024-09-11; ransomware use Unknown

Problem Types: CWE-287

CISA Known Exploited Vulnerability

Vendor	Dahua
Product	IP Camera Firmware
Name	Dahua IP Camera Authentication Bypass Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://www.dahuasecurity.com/aboutUs/trustedCenter/details/582 ; https://nvd.nist.gov/vuln/detail/CVE-2021-33045

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dahuasecurity	lpc-hum7xxx	-	All	All	All
Operating System	Dahuasecurity	lpc-hum7xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	lpc-hx3xxx	-	All	All	All
Operating System	Dahuasecurity	lpc-hx3xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	lpc-hx5xxx	-	All	All	All
Operating System	Dahuasecurity	lpc-hx5xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	Nvr-1xxx	-	All	All	All

Operating System	Dahuasecurity	Nvr-1xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	Nvr-2xxx	-	All	All	All
Operating System	Dahuasecurity	Nvr-2xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	Nvr-4xxx	-	All	All	All
Operating System	Dahuasecurity	Nvr-4xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	Nvr-5xxx	-	All	All	All
Operating System	Dahuasecurity	Nvr-5xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	Nvr-6xx	-	All	All	All
Operating System	Dahuasecurity	Nvr-6xx Firmware	All	All	All	All
Hardware	Dahuasecurity	Vth-542xh	-	All	All	All
Operating System	Dahuasecurity	Vth-542xh Firmware	All	All	All	All
Hardware	Dahuasecurity	Vto-65xxx	-	All	All	All
Operating System	Dahuasecurity	Vto-65xxx Firmware	All	All	All	All
Hardware	Dahuasecurity	Vto-75x95x	-	All	All	All
Operating System	Dahuasecurity	Vto-75x95x Firmware	All	All	All	All
Hardware	Dahuasecurity	Xvr-4x04	-	All	All	All
Operating System	Dahuasecurity	Xvr-4x04 Firmware	All	All	All	All
Operating System	Dahuasecurity	Xvr-4x04 Firmware	-	All	All	All
Hardware	Dahuasecurity	Xvr-4x08	-	All	All	All
Operating System	Dahuasecurity	Xvr-4x08 Firmware	All	All	All	All
Hardware	Dahuasecurity	Xvr-5x04	-	All	All	All
Operating System	Dahuasecurity	Xvr-5x04 Firmware	All	All	All	All
Hardware	Dahuasecurity	Xvr-5x08	-	All	All	All
Operating System	Dahuasecurity	Xvr-5x08 Firmware	All	All	All	All
Hardware	Dahuasecurity	Xvr-5x16	-	All	All	All
Operating System	Dahuasecurity	Xvr-5x16 Firmware	All	All	All	All
Hardware	Dahuasecurity	Xvr-7x16	-	All	All	All
Operating System	Dahuasecurity	Xvr-7x16 Firmware	All	All	All	All
Hardware	Dahuasecurity	Xvr-7x32	-	All	All	All
Operating System	Dahuasecurity	Xvr-7x32 Firmware	All	All	All	All

References

Reference	Source	Link	Tag
Dahua Authentication Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	
Full Disclosure: [Update]: Dahua Authentication bypass (CVE-2021-33044, CVE-2021-33045)	FULLDISC	seclists.org	
Security Advisory - Identity authentication bypass vulnerability found in some Dahua products	MISC	www.dahuasecurity.com	

CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)