



# CVE-2020-5735

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-5735
<b>State</b>	PUBLIC
<b>Assigner</b>	vulnreport@tenable.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-08 13:15:00 UTC
<b>Updated</b>	2020-04-09 19:52:00 UTC
<b>Description</b>	Amcrest cameras and NVR are vulnerable to a stack-based buffer overflow over port 37777. An authenticated remote attac

## Risk And Classification

**EPSS:** 0.613690000 probability, percentile 0.983100000 (date 2026-04-02)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-787

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Amcrest
<b>Product</b>	Cameras and Network Video Recorder (NVR)
<b>Name</b>	Amcrest Cameras and NVR Stack-based Buffer Overflow Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-5735">https://nvd.nist.gov/vuln/detail/CVE-2020-5735</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Amcrest</a>	<a href="#">1080-lite 8ch</a>	-	All	All	All
Hardware	<a href="#">Amcrest</a>	<a href="#">1080-lite 8ch</a>	-	All	All	All
Operating System	<a href="#">Amcrest</a>	<a href="#">1080-lite 8ch Firmware</a>	-	All	All	All
Operating System	<a href="#">Amcrest</a>	<a href="#">1080-lite 8ch Firmware</a>	-	All	All	All
Hardware	<a href="#">Amcrest</a>	<a href="#">Amdv10814-h5</a>	-	All	All	All
Hardware	<a href="#">Amcrest</a>	<a href="#">Amdv10814-h5</a>	-	All	All	All
Operating System	<a href="#">Amcrest</a>	<a href="#">Amdv10814-h5 Firmware</a>	-	All	All	All
Operating System	<a href="#">Amcrest</a>	<a href="#">Amdv10814-h5 Firmware</a>	-	All	All	All

Hardware	Amcrest	Ip2m-841	-	All	All	All
Hardware	Amcrest	Ip2m-841	-	All	All	All
Hardware	Amcrest	Ip2m-841-v3	-	All	All	All
Hardware	Amcrest	Ip2m-841-v3	-	All	All	All
Operating System	Amcrest	Ip2m-841-v3 Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-841-v3 Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-841 Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-841 Firmware	All	All	All	All
Hardware	Amcrest	Ip2m-853ew	-	All	All	All
Hardware	Amcrest	Ip2m-853ew	-	All	All	All
Operating System	Amcrest	Ip2m-853ew Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-853ew Firmware	All	All	All	All
Hardware	Amcrest	Ip2m-858w	-	All	All	All
Hardware	Amcrest	Ip2m-858w	-	All	All	All
Operating System	Amcrest	Ip2m-858w Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-858w Firmware	All	All	All	All
Hardware	Amcrest	Ip2m-866ew	-	All	All	All
Hardware	Amcrest	Ip2m-866ew	-	All	All	All
Operating System	Amcrest	Ip2m-866ew Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-866ew Firmware	All	All	All	All
Hardware	Amcrest	Ip2m-866w	-	All	All	All
Hardware	Amcrest	Ip2m-866w	-	All	All	All
Operating System	Amcrest	Ip2m-866w Firmware	All	All	All	All
Operating System	Amcrest	Ip2m-866w Firmware	All	All	All	All
Hardware	Amcrest	Ip4m-1053ew	-	All	All	All
Hardware	Amcrest	Ip4m-1053ew	-	All	All	All
Operating System	Amcrest	Ip4m-1053ew Firmware	All	All	All	All
Operating System	Amcrest	Ip4m-1053ew Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-2454ew	-	All	All	All
Hardware	Amcrest	Ip8m-2454ew	-	All	All	All
Operating System	Amcrest	Ip8m-2454ew Firmware	All	All	All	All
Operating System	Amcrest	Ip8m-2454ew Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-2493eb	-	All	All	All
Hardware	Amcrest	Ip8m-2493eb	-	All	All	All
Operating System	Amcrest	Ip8m-2493eb Firmware	All	All	All	All

Operating System	Amcrest	Ip8m-2493eb Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-2496eb	-	All	All	All
Hardware	Amcrest	Ip8m-2496eb	-	All	All	All
Operating System	Amcrest	Ip8m-2496eb Firmware	All	All	All	All
Operating System	Amcrest	Ip8m-2496eb Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-2597e	-	All	All	All
Hardware	Amcrest	Ip8m-2597e	-	All	All	All
Operating System	Amcrest	Ip8m-2597e Firmware	All	All	All	All
Operating System	Amcrest	Ip8m-2597e Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-mb2546ew	-	All	All	All
Hardware	Amcrest	Ip8m-mb2546ew	-	All	All	All
Operating System	Amcrest	Ip8m-mb2546ew Firmware	All	All	All	All
Operating System	Amcrest	Ip8m-mb2546ew Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-mt2544ew	-	All	All	All
Hardware	Amcrest	Ip8m-mt2544ew	-	All	All	All
Operating System	Amcrest	Ip8m-mt2544ew Firmware	All	All	All	All
Operating System	Amcrest	Ip8m-mt2544ew Firmware	All	All	All	All
Hardware	Amcrest	Ip8m-t2499ew	-	All	All	All
Hardware	Amcrest	Ip8m-t2499ew	-	All	All	All
Operating System	Amcrest	Ip8m-t2499ew Firmware	All	All	All	All
Operating System	Amcrest	Ip8m-t2499ew Firmware	All	All	All	All
Hardware	Amcrest	Ipm-721	-	All	All	All
Hardware	Amcrest	Ipm-721	-	All	All	All
Operating System	Amcrest	Ipm-721 Firmware	All	All	All	All
Operating System	Amcrest	Ipm-721 Firmware	All	All	All	All
Hardware	Amcrest	Ipm-hx1	-	All	All	All
Hardware	Amcrest	Ipm-hx1	-	All	All	All
Operating System	Amcrest	Ipm-hx1 Firmware	All	All	All	All
Operating System	Amcrest	Ipm-hx1 Firmware	All	All	All	All

## References

Reference	Source	Link	Tags
Amcrest Camera/NVR Multiple Vulnerabilities - Research Advisory   Tenable®	MISC	<a href="http://www.tenable.com">www.tenable.com</a>	Third Party Advisory
Amcrest Dahua NVR Camera IP2M-841 Denial Of Service ≈ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>	Exploit, Third Party
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**