



CVE-2021-31986

Published on: 10/05/2021 12:00:00 AM UTC

Last Modified on: 10/13/2021 08:18:00 PM UTC

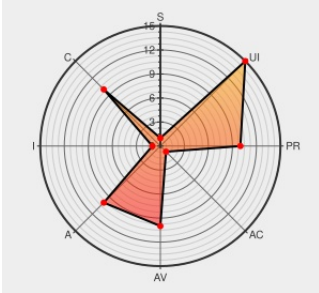
CVE-2021-31986

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:H



Certain versions of [Axis Os](#) from [Axis](#) contain the following vulnerability:

User controlled parameters related to SMTP notifications are not correctly validated. This can lead to a buffer overflow resulting in crashes and data leakage.

CVE-2021-31986 has been assigned by product-security@axis.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
	www.axis.com/application/pdf	MISC www.axis.com/files/tech_notes/CVE-2021-31986.pdf

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
Operating System	Axis	Axis Os	All	All	All	All
Operating System	Axis	Axis Os 2016	All	All	All	All
Operating System	Axis	Axis Os 2018	All	All	All	All
Operating System	Axis	Axis Os 2020	All	All	All	All

cpe:2.3:o:axis:axis_os:*:*:*:active:*:*:

cpe:2.3:o:axis:axis_os_2016:*:*:*:its:*:*:

cpe:2.3:o:axis:axis_os_2018:*:*:*:its:*:*:

cpe:2.3:o:axis:axis_os_2020:*:*:*:its:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @Cyber_O51NT	Nozomi found three new vulnerabilities (CVE-2021-31986, CVE-2021-31987, CVE-2021-31988) affecting all Axis devices... twitter.com/i/web/status/1...	2021-10-06 09:59:39
 @STechForum	#vulnerability #surveillance Axis IP Video Surveillance Systems Vulnerable (CVE-2021-31986) sensorstechforum.com/axis-ip-video-... https://t.co/jDcEFMWUpg	2021-10-06 10:32:33
 @foxbook	「3つのバグ (CVE-2021-31986、 CVE-2021-31987、 CVE-2021-31988) が、会社の組み込み AxisOSを実行するすべてのAxisデバイスに影響を与えることが判明した」 「 Axis GearのIP監... twitter.com/i/web/status/1...	2021-10-06 21:17:37

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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](#).

