

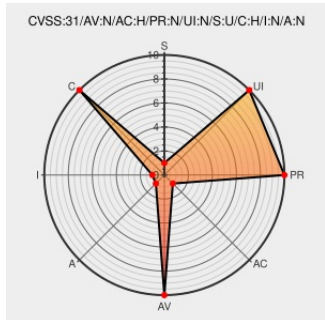


CVE-2020-3929

Published on: 06/12/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-3929

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Geovision Gv-as1010](#) from [Usavisionsys](#) contain the following vulnerability:

GeoVision Door Access Control device family employs shared cryptographic private keys for SSH and HTTPS. Attackers may conduct MITM attack with the derived keys and plaintext recover of encrypted messages.

CVE-2020-3929 has been assigned by cve@cert.org.tw to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [GeoVision](#) - **Door Access Control Device** version ≤ 2.21

Affected Vendor/Software: [GeoVision](#) - **Door Access Control Device** version ≤ 2.21

Affected Vendor/Software: [GeoVision](#) - **Door Access Control Device** version ≤ 2.21

Affected Vendor/Software: [GeoVision](#) - **Door Access Control Device** version ≤ 1.10

Affected Vendor/Software: [GeoVision](#) - **Door Access Control Device** version ≤ 1.32

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description

Tags

Link

TWCERT/CC台灣電腦網路危機處理暨協調中心-GeoVision 門禁控制設備 - Shared cryptographic keys

Third Party Advisory
[www.twcert.org.tw
text/html](http://www.twcert.org.tw/text/html)

 MISC www.twcert.org.tw/tw/cp-132-3696-6601c-1.html

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 	Usavisionsys	Geovision Gv-as1010	-	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as1010	-	All	All	All
Operating System	Usavisionsys	Geovision Gv-as1010 Firmware	All	All	All	All
Operating System	Usavisionsys	Geovision Gv-as1010 Firmware	All	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as210	-	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as210	-	All	All	All
Operating System	Usavisionsys	Geovision Gv-as210 Firmware	All	All	All	All
Operating System	Usavisionsys	Geovision Gv-as210 Firmware	All	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as410	-	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as410	-	All	All	All
Operating System	Usavisionsys	Geovision Gv-as410 Firmware	All	All	All	All
Operating System	Usavisionsys	Geovision Gv-as410 Firmware	All	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as810	-	All	All	All
Hardware 	Usavisionsys	Geovision Gv-as810	-	All	All	All
Operating System	Usavisionsys	Geovision Gv-as810 Firmware	All	All	All	All
Operating System	Usavisionsys	Geovision Gv-as810 Firmware	All	All	All	All
Hardware 	Usavisionsys	Geovision Gv-gf192x	-	All	All	All

Hardware 	Usavisionsys	Geovision Gv-gf192x	-	All	All	All
Operating System	Usavisionsys	Geovision Gv-gf192x Firmware	All	All	All	All
Operating System	Usavisionsys	Geovision Gv-gf192x Firmware	All	All	All	All
cpe:2.3:h:usavisionsys:geovision_gv-as1010:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as1010:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as1010_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as1010_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as210:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as210:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as210_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as210_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as410:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as410:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as410_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as410_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as810:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-as810:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as810_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-as810_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-gf192x:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:usavisionsys:geovision_gv-gf192x:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-gf192x_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:usavisionsys:geovision_gv-gf192x_firmware:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)