GeoVision

Home > Cyber Security

CYBER SECURITY

GeoVision's Cyber Security Policy

Overview

Security First at GeoVision

It is the duty and responsibility of GeoVision to notify all users in cases when security concerns have been raised. GeoVision follows detailed practices to ensure the highest standards of network security are met. Whenever plausible security vulnerabilities are discovered, immediate actions are taken by devising necessary upgrades and informing users of the issues.

GeoVision is the first Taiwan tech company to be certified by TAICS (Taiwan Association of Information and Communication Standards), on 2018/11/19, to pass its Level 2 of video surveillance system security standards. As of date, it is the highest level of security any Taiwan tech company has achieved.

The latest security patches and updates are included in the latest software/firmware releases and are available at GeoVision product download page at https://www.geovision.com.tw/download/product/ provided the product is still supported by GeoVision.

Contact Information

We encourage users to report any newly discovered vulnerability in our products by contacting our security team at security@geovision.com.tw

GeoVision Vulnerability Policy

Vulnerability Management Flow

For any newly reported vulnerability in any GeoVision product, a specific team is dispatched to work with research & development and testing departments and ensure the solution is provided without generating any further risk to users.

The main general flow is designed in 4 stages:

- Discover
- Analyze
- Prioritize
- Solution update & follow up

Vulnerability Classification

A vulnerability when confirmed is classified as non-critical or critical.

The class of critical would suggest high level of risk for users and GeoVision will provide an unscheduled update to fix the vulnerability and documentation to assist users on applying the update.

The Non-critical class vulnerability when not posing any risk to the recommended usage of the product is going to be solved in the normally scheduled firmware release.

Processing and Reaction Time

Any valid report sent to security@geovision.com.tw will be responded within 48 hours and with the possibility of additional questions required for investigation.

Certifications

TAICS (Taiwan Association of Information and Communication Standards)

- GeoVision certified product list

CVE Publication

Disclosure Policy

When we assign a CVE, our goal is to publish CVE details within one week of confirming the vulnerability. CVE details may be published before fixes are available.
Wherever possible, we aim to coordinate disclosure with reporters. Upon request, we are happy to publicly acknowledge reporters on our cybersecurity webpage.

Security Advisory

Advisory ID	Advisory	CVE ID	Status	Date Published	Article
GV-ERM-2026-03-01	GV-Edge Recording Manager Vulnerability	CVE-2026-4606	Completed	23-Mar-26	Security Advisory
GV-ASM-2025-04-01	GV-ASManager Web Vulnerabilities	CVE-2025-26263 CVE-2025-26264	Completed	9-Apr-25	Security Advisory
GV-ASM-2025-02-03	GV-ASManager Web Vulnerabilities	CVE-2024-56898 CVE-2024-56901 CVE-2024-56902 CVE-2024-56903	Completed	3-Feb-25	Security Advisory
GV-ASM-2024-12-13	GV-ASManager Web Vulnerabilities	CVE-2024-12553	Completed	13-Dec-24	Security Advisory
GV-IP-2024-11-1	EOL IP devices OS injection vulnerabilities	CVE-2024-6047, CVE-2024-11120	Completed	20-Nov-24	Security Advisory
GV-IP-2023-07-1	GV-ADR2701 Login response vulnerability	CVE-2023-3638	Completed	19-Jul-23	Security Advisory
GV-ERM-2023-05	GV-Edge Recording Manager (Windows) Vulnerabilities	CVE-2023-23059	Completed	03-May-23	Security Advisory
GV-ASM-	GV-ASManager Vulnerabilities	N/A	Completed	23-Nov-22	Security

Advisory ID	Advisory	CVE ID	Status	Date Published	Article
GV-IP-2022-04	Statement of Passwords	N/A	Completed	11-Apr-22	Statement of Passwords
GV-SFW-2022-01	Notice of Log4j Vulnerabilities	CVE-2021-44228, CVE-2021-45046	Completed	6-Jan-22	Notice of Log4j Vulnerabilities
GV-Cloud-2021-10	Notice of Security Incident	N/A	Completed	22-Oct-21	Notice of Security Incident
GV-IP-2021-09	IP Camera Vulnerabilities	N/A	Completed	28-Sep-21	Security Advisory
GV-IP-2021-07	IP Camera Vulnerabilities	N/A	Completed	27-Sep-21	Security Advisory
GV-ASM-2021-06	Multiple XSS Vulnerabilities	N/A	Completed	21-Jul-21	Security Advisory
GV-Cloud-2020-09	myGVcloud XSS & CSRF Vulnerabilities	N/A	Completed	21-Sep-20	N/A