GVision Italia S.r.l.

Terminal Manufacturer for EU Market
Via Prealpi 14, 20833 Giussano (MB), Italy
P.IVA: IT10412540964 · Tel: +39 02 87187733

GVSA-2025-002

Published: February 3, 2025

RESOLVED

Security Advisory: Multiple Vulnerabilities in GV-ASManager Web Application

EXECUTIVE SUMMARY

Multiple security vulnerabilities have been identified in the GeoVision ASManager web application (ASWeb component) affecting access control, authentication, and information disclosure. These vulnerabilities could lead to privilege escalation, unauthorized account creation, and credential exposure. GVision Italia, as Terminal Manufacturer for the EU market, has coordinated the patch distribution and provided enhanced security configurations for European deployments.

⚠ IMPORTANT SECURITY UPDATE

Multiple vulnerabilities with combined CVSS scores ranging from 6.5 to 8.8. Immediate update to version 6.2.0 or later is strongly recommended.

VULNERABILITY SUMMARY

CVE ID	Type	CVSS v3.1	Severity
CVE-2024-56898	Broken Access Control	8.8	HIGH
CVE-2024-56901	Cross-Site Request Forgery	8.1	HIGH
CVE-2024-56902	Information Disclosure	6.5	MEDIUM
CVE-2024-56903	Request Method Tampering	7.5	HIGH

AFFECTED SOFTWARE

Product: GeoVision ASManager Web Application (ASWeb)
Component: Web Management Interface
Affected Versions:
• Version 6.1.1.0 and earlier (CVE-2024-56901, 56902, 56903)
• Version 6.1.0.0 and earlier (CVE-2024-56898)
Fixed Version: Version 6.2.0

Associated Modules:
• ASWeb - Access & Security Management
• TAWeb - Time and Attendance Management
• VMWeb - Visitor Management

TECHNICAL DETAILS

CVE-2024-56898 - Broken Access Control (CVSS 8.8):
Low-privilege users can perform unauthorized actions including creating, modifying, or deleting accounts. The Guest account (enabled by default) can escalate privileges to administrator level.

CVE-2024-56901 - Cross-Site Request Forgery (CVSS 8.1):

Lack of CSRF tokens allows attackers to create administrator accounts through crafted requests when combined with CVE-2024-56903.

CVE-2024-56902 - Information Disclosure (CVSS 6.5):
Cleartext passwords can be retrieved from the application, potentially leading to credential reuse attacks across the organization.

CVE-2024-56903 - Request Method Tampering (CVSS 7.5):
POST requests can be converted to GET requests in critical functionalities, enabling CSRF attacks when chained with CVE-2024-56901.

TERMINAL MANUFACTURER SECURITY ENHANCEMENTS

GVision Italia has implemented EU-specific security configurations for deployments in critical infrastructure:

- **Default Account Hardening:** Guest account disabled by default in EU distributions
- **NIS2 Compliance:** Enhanced audit logging and session management
- **Access Control:** Mandatory role-based access control (RBAC) templates
- **Password Policy:** Enforced complexity requirements per EU standards
- **Network Segmentation:** Configuration guides for isolated deployment

RESOLUTION

URGENT - Required Actions:

1. **Immediately disable** Guest account if enabled
2. Audit all user accounts for unauthorized modifications
3. Update GV-ASManager to version 6.2.0 or later
4. Reset all user passwords after update
5. Review access logs for suspicious activity
6. Implement network segmentation if not already in place

> **EU Compliance Package:** A comprehensive security configuration package (GV-ASManager-EU-Security-Config.tar) is available for organizations requiring NIS2 and Cyber Resilience Act compliance documentation.

DISCLOSURE TIMELINE

January 8, 2025: Vulnerabilities discovered by Giorgi Dograshvili

January 10, 2025: Reported to GeoVision Inc. via responsible disclosure

January 11, 2025: GVision Italia notified as EU Terminal Manufacturer

January 20, 2025: Patches developed and testing initiated

January 28, 2025: EU security configurations completed

February 2, 2025: Exploit code published on Exploit-DB

February 3, 2025: Emergency public disclosure

MITIGATION RECOMMENDATIONS

For organizations unable to immediately update:

- Disable Guest account immediately
- Restrict ASWeb access to trusted IP addresses only

- Implement Web Application Firewall (WAF) rules
- Monitor authentication logs for anomalies
- Enable multi-factor authentication where possible

CREDITS & REFERENCES

Discovery: Giorgi Dograshvili (DRAGOWN)
CVE Assignment: GeoVision Inc. CNA
EU Coordination: GVision Italia S.r.l.
Public Exploits:

- Exploit-DB #52187 (CSRF)
- Exploit-DB #52189 (Access Control)
- GitHub: DRAGOWN/CVE-2024-56898
- GitHub: DRAGOWN/CVE-2024-56901
- GitHub: DRAGOWN/CVE-2024-56902
- GitHub: DRAGOWN/CVE-2024-56903

Authorized and Approved by:

Alberto Patella

Founder & Chief Executive Officer
Terminal Manufacturer Representative
ISO/IEC 27001:2022 Lead Implementer

CTU - Court Technical Expert, Tribunals of Brescia and Milano
Professor of Applied Criminology, University of Bologna
Cruz Blanca al Valor Policial - Spanish Guardia Civil

24/7 Security Hotline: +39 02 87187733
Emergency Email: security@gvision.it
Advisory URL: https://www.gvision.it/security/advisories/2025/GVSA-2025-002
Security Configuration Package: Available upon request for EU customers

This security advisory is published under ISO/IEC 29147:2018 guidelines
Compliant with NIS2 Directive (EU) 2022/2555 and Cyber Resilience Act (EU) 2024/2847
Distribution is unlimited - Immediate action recommended