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-2025-001

Published: April 9, 2025

RESOLVED

Security Advisory: GV-ASManager Software Vulnerabilities

EXECUTIVE SUMMARY

Multiple security vulnerabilities have been identified in the GeoVision ASManager software (Windows desktop application) affecting authentication and session management components. As the appointed Terminal Manufacturer for the European Union market, GVision Italia has coordinated the patch distribution and provided additional security guidance for EU deployments.

VULNERABILITY DETAILS

Severity:	HIGH	**Impact:**	**Critical**
Vector:	**Network/Local**	**Complexity:**	**Low**

CVE Identifiers:

CVE-2025-26263 CVE-2025-26264

AFFECTED SOFTWARE

Product: GeoVision ASManager (Windows Application)
Component: ASManagerService.exe and ASWeb Interface
Affected Versions: Version 6.1.2.0 and earlier
Fixed Version: Version 6.2.0

Vulnerability Types:
• CVE-2025-26263: Credential Disclosure (memory handling issue)
• CVE-2025-26264: Remote Code Execution (notification settings)

TECHNICAL DETAILS

CVE-2025-26263 - Credential Disclosure:
The ASManagerService.exe process improperly handles memory, potentially exposing credentials in clear text. This vulnerability requires local access to the system.

CVE-2025-26264 - Remote Code Execution:
The ASWeb interface contains an RCE vulnerability in the Notification Settings feature. An authenticated attacker with System Settings privileges can execute arbitrary commands on the server, leading to complete system compromise.

TERMINAL MANUFACTURER ACTIONS

GVision Italia, as Terminal Manufacturer for EU market distribution, has implemented the following measures:

- Coordinated patch testing in EU operational environments
- Validated software update against EU regulatory requirements
- Prepared deployment guidelines for critical infrastructure installations
- Created hardening checklist specific to NIS2 compliance
- Established monitoring procedures for post-patch verification

RESOLUTION

Immediate Action Required:

1. Update GV-ASManager to version 6.2.0 or later
2. Download from GeoVision official site or GVision Italia portal
3. Stop ASManagerService.exe before update
4. Apply update during maintenance window
5. Verify successful installation via Help → About
6. Review audit logs for any suspicious activity

EU-Specific: For installations in critical infrastructure, contact GVision Italia for deployment support and compliance documentation.

DISCLOSURE TIMELINE

March 15, 2025:	Vulnerabilities reported to GeoVision Inc.
March 18, 2025:	GVision Italia notified as EU Terminal Manufacturer
March 25, 2025:	Patch developed by GeoVision Inc.
April 5, 2025:	EU deployment testing completed
April 9, 2025:	Coordinated public disclosure

CREDITS

Discovery: Giorgi Dograshvili (DRAGOWN)
Vendor Response: GeoVision Inc. Security Team
EU Coordination: GVision Italia S.r.l.
CVE Assignment: GeoVision Inc. CNA (CNA-2020-0005)

Authorized by:

Alberto Patella

Founder & Chief Executive Officer
Terminal Manufacturer Representative

CTU - Court Technical Expert, Tribunals of Brescia and Milano
Professor of Applied Criminology, University of Bologna
Cruz Blanca al Valor Policial - Spanish Guardia Civil
ISO/IEC 27001:2022 Lead Implementer

Security Contact: security@gvision.it
Phone: +39 02 87187733
Advisory URL: https://www.gvision.it/security/advisories/2025/GVSA-2025-001
GeoVision Advisory:
https://dlcdn.geovision.com.tw/TechNotice/CyberSecurity/Security_Advisory_GV-ASManager-2025-04-09.pdf