

## Security Advisory MIDEA-SA-2026-001

### 1. Description

A vulnerability has been identified in the Midea Smart Air Conditioner Controller. The issue allows an attacker to bypass authentication by sending specially crafted requests, potentially gaining unauthorized access to device control interfaces.

---

### 2. Vulnerability Identifier

- Internal ID: MIDEA-SA-2026-001
  - CVE ID: CVE-2026-XXXX (if assigned)
- 

### 3. Affected Products

The following products and versions are affected:

Product Name	Model	Firmware Version
Smart AC Controller	MSAC-1000	≤ v1.2.3
Smart AC Controller Pro	MSAC-2000	≤ v2.0.1

Only devices running the above versions are impacted.

---

### 4. Impact

Successful exploitation of this vulnerability may result in:

- Unauthorized remote control of the device
  - Exposure of user data or sensitive information
  - Potential use of the device in broader network attacks (e.g., botnets)
- 

### 5. Severity

- **CVSS v3.1 Score:** 8.8 (High)
  - **Severity Level:** High
-

## 6. Remediation

Midea has released fixed firmware versions. Users are strongly advised to upgrade as soon as possible.

### ✓ Fixed Versions:

- MSAC-1000 → v1.2.4 and later
- MSAC-2000 → v2.0.2 and later

### ✓ Upgrade Steps:

1. Open the Midea Smart App
2. Navigate to the device management section
3. Check for firmware updates
4. Download and install the latest version

### ✓ Temporary Mitigation (if upgrade is not immediately possible):

- Disable remote access features
  - Restrict device access to trusted networks
- 

## 7. Release Date

June 1, 2026

---

## 8. Last Updated

June 1, 2026

---

## 9. Acknowledgement

Midea would like to thank the security researcher **[Researcher Name]** for responsibly reporting this issue.

---

## 10. Contact

For security-related inquiries, please contact: [iotsecurity@midea.com](mailto:iotsecurity@midea.com)