

SECURITY ADVISORY

Vulnerability in ARMATURA ONE

Advisory Reference	CERT/CC VU#855730
Date	2026-09-14
Affected Product	Armatura ONE V4.3.1_USA and all earlier USA versions
Fixed Version	AONE V4.6.1_USA
Recommended Action	Upgrade as soon as possible

Dear Valued Customer,

Security vulnerabilities have been identified affecting Armatura ONE V4.3.1_USA and earlier versions. We are notifying you so you can take prompt action to protect your system. A fixed version is now available, and we strongly recommend that all affected customers upgrade as soon as possible.

1. Affected Versions

Armatura ONE V4.3.1_USA and all earlier USA versions.

2. Vulnerability Summary

- **Access Control:** A flaw in access control could allow an attacker to gain unauthorized access to system resources.
- **Encryption and Key Management:** A weakness in encryption and key management could allow an attacker to bypass the credential obfuscation mechanism.
- **Information Disclosure:** An information leakage issue could allow an attacker to obtain credentials without authorization.

3. Recommended Actions

1. **Restrict access before upgrading:** Until the upgrade is complete, reduce exposure by disabling externally accessible network ports and limiting system access to authorized personnel only.
2. **Back up your data:** Create a complete backup of all system data before upgrading to prevent data loss.
3. **Upgrade the software:** Upgrade to AONE V4.6.1_USA, which resolves these vulnerabilities.
4. **Obtaining the Update**

To obtain the patch package for AONE V4.6.1_USA please visit [AONE V4.6.1 downloads](#), or contact info@zktecousa.com.

We appreciate your prompt attention to this matter and remain committed to the security of your systems. If you have any questions or need assistance with the upgrade, please contact our support team at support@zktecousa.com.

Thank you.