

Notice Regarding Security Vulnerability in Armatura ONE

Dear Valued Customers,

This notice is to inform you of a security vulnerability identified in USA versions Armatura ONE V4.3.1_USA or earlier versions and mainstream versions Armatura One V4.7.1 or earlier versions. It is essential to take the necessary actions to protect your systems for your attention to this matter.

1. Vulnerability Details

Vulnerability : VU#855730

Scope of Impact: For USA versions, Armatura ONE V4.3.1_USA and earlier versions. For Mainstream versions, Armatura ONE V4.7.1 and earlier versions.

Vulnerability Overview:

- A. An access control vulnerability exists: successful exploitation could lead to unauthorized access to system resources.
- B. An encryption and key management vulnerability exists: successful exploitation could compromise the credential confusion mechanism.
- C. An information leakage vulnerability exists: successful exploitation could result in unauthorized acquisition of credentials.

2. Vulnerability Solution

Address: 1600 Union Hill Road Alpharetta Georgia 30005
Company website: armatura.us; Email: info@armatura.us

- A. Software upgrade: For USA versions, please upgrade to Armatura ONE V4.6.1_USA. For Mainstream versions, please upgrade to Armatura ONE V4.7.2.
- B. Enhance security level: Before performing the upgrade, ensure that the system has implemented all necessary protective measures, such as disabling external network ports or restricting access permissions.
- C. Back up data: Before proceeding with the upgrade, make sure to back up all relevant data to prevent data loss.

3. Contact Information

- A. Please contact info@armatura.us to obtain the patch package for the fixed version.
- B. You may also contact the Armatura branch in your region to obtain the patch package for the repaired version.