Date: 06/30/2017

Ampla Security Bulletin LFSEC00000118

Title

Ampla MES multiple vulnerabilities

Rating

Medium

Published By

Ampla|Schneider Electric Security Response Center

Overview

Ampla by Schneider Electric has created a security update to address vulnerabilities in the **Ampla MES versions 6.4 and prior**. The vulnerabilities, if exploited, could allow a malicious entity to:

- Compromise credentials used to connect to 3rd party databases
- Compromise credentials of Ampla Users configured with Simple Security

Schneider Electric recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

This security bulletin announces the software security update for the **Ampla MES versions 6.4 and prior.**

Recommendations

Customers using **Ampla MES versions 6.4 and prior** are affected and should upgrade to **Ampla MES version 6.5** as soon as possible.

Background

Ampla MES is a Manufacturing Execution System that drives operational efficiency. Ampla MES is used in many industries worldwide, including manufacturing, mining, water and wastewater management.

To identify the version of Ampla you have installed, navigate to Windows Programs and Features, locate “Schneider Electric Ampla” installation and look at the version. If you are running Ampla 6.4.* and lower, you are using a vulnerable version.

Vulnerability Details

1) Ampla MES provides capability to interact with data from 3rd party databases. When connectivity to those databases is configured to use a SQL user name and password, an Information Disclosure vulnerability could result in the connection string details being leaked. Note that when the 3rd party database connectivity is configured with Windows Integrated Security as opposed to SQL username and password, the software is not vulnerable.

2) Ampla MES provides capability to configure users and their privileges. When Ampla MES users are configured to use Simple Security, a weakness in the password hashing algorithm could be exploited to reverse the user's password. Note that when Ampla MES is configured to use Windows Integrated Security as opposed to Simple Security, the software is not vulnerable.

Security Update

The following Security Update addresses the vulnerabilities outlined in this Security Bulletin.
June 30, 2017: Ampla MES version 6.5

Affected Products, Components, and Corrective Security Patches

The following table identifies the currently supported products affected. Software updates can be downloaded from Ampla Support "Shopping Kiosk" area or from the links below:

Product and Component	Supported Operating System	Security Impact	Severity Rating	Software Security Update
Ampla MES version 6.4 and prior	Multiple	Confidentiality	Medium	Ampla MES 6.5

Additional Recommendations

For an increased level of security, Schneider Electric recommends configuring and running Ampla MES with Windows Integrated Security as opposed to SQL Native Logins and Ampla Simple Security.

Vulnerability Characterization and CVSSv3 Rating

CWE-312: Cleartext Storage of Sensitive Information, CWE-916: Use of Password Hash with Insufficient Computational Effort

- Ampla MES credential leakage **6.7** | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
- Ampla MES password reversal **4.2** | CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

Acknowledgements

Schneider Electric would like to thank:

- **Ilya Karpov** from **Positive Technologies** for the discovery, responsible disclosure of this vulnerability, and verification of the security fixes in Ampla MES 6.5
- **ICS-Cert** for coordination of advisories

Support

For information on how to reach Schneider Electric support for your product, please refer to this link: Schneider Electric Software Global Customer Support.

If you discover errors or omissions in this Security Notification, please report the finding to Support.

Schneider Electric Software Security Updates

For the latest security information and security updates, please visit SE Security Updates.

Cyber Security Standards and Best Practices

For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

NVD Common Vulnerability Scoring System (CVSS v3)

The U.S. Department of Homeland Security has adopted the common Vulnerability Scoring System (CVSS v3) that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v3 produces a numerical score as well as a textual representation of that score reflecting the severity of a vulnerability. Scores range from 0.0 (no impact) to a maximum of 10.0 (critical impact with minimal effort to exploit). For additional information please refer to the CVSSv3 specifications.

Disclaimer