ABB DOC ID: 9AKK107046A5821
REVISION: -
DATE: 2018-08-10

CYBER SECURITY ADVISORY

eSOMS LDAP Integration

ABBVU-PGGA-2018030

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

eSOMS 6.0.2

Vulnerability ID

ABB ID: ABBVU-PGGA-2018030

Summary

An issue exists in eSOMS version 6.0.2 configured with LDAP authentication where a user can log into the application with a blank password. The issue is caused by a feature in LDAP that allows anonymous authentication, along with a misconfigured web.config file in eSOMS. Both cases must exist for the issue to be present.

An attacker who successfully exploited this vulnerability could gain access to the application as a valid user. The attacker would have to discover the account username.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3 Base Score:	9.8 (Critical)
CVSS v3 Temporal Score:	8.0 (Critical)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C

Recommended immediate actions

Customers running eSOMS version 6.0.2 should ensure "Unauthenticated Authentication" (anonymous bind) is disabled in the LDAP configuration settings. In the eSOMS web.config file, ensure only the following key values are populated: "LDAP_Path", "LDAP_User_Search" and "LDAP_SSL_Enabled". The remaining LDAP related key values are reserved for non-standard LDAP server configurations and are not normally required.

Please contact Global Customer Care (GCC) for further guidance if you run into issues implementing LDAP authentication using only the previously mentioned key values.

This issue will be resolved in eSOMS 6.0.3 by adding a check to prevent a user from authenticating to eSOMS with a blank password regardless of the LDAP server or web.config settings.

Vulnerability Details

LDAP authentication servers can be configured to allow anonymous authentication. When configuring LDAP authentication within eSOMS, a user can login with a blank password if the following settings are configured:

1. LDAP server is configured to allow “Unauthenticated Authentication”

2. The eSOMS web.config LDAP related keys **other than** “LDAP_Path”, “LDAP_User_Search” and “LDAP_SSL_Enabled” are populated with valid values

Mitigating Factors

Industry accepted security best practices for a defense in depth strategy can help mitigate many common risk scenarios. Such practices include appropriate physical controls to protect systems from direct access by unauthorized personnel, ensuring no direct connections to the Internet, and proper network segmentation using a firewall configured to allow only required ports and services. Additional ports should be evaluated on a case by case basis. Application systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to the network. Users should regularly receive education on the proper usage of resources and the importance of security practices

Workarounds

See “Recommended Immediate Actions” section.

Frequently Asked Questions

What causes the vulnerability?

The vulnerability is caused by a misconfigured LDAP server that allows anonymous authentication along with a misconfigured eSOMS web.config file.

What is the <affected product or component>?

eSOMS 6.0.2 web application.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain access to the application as a legitimate user.

How could an attacker exploit the vulnerability?

An attacker would need to discover valid usernames and have network access to the eSOMS application.

Could the vulnerability be exploited remotely?

Yes, if authentication requests cross a network boundary an attacker would be able to exploit this vulnerability remotely.

What does the update do?

The update adds a check to prevent a user from being able to authenticate with a blank password.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.