ABB DOC ID: 9AKK107492A9964
REVISION: B
DATE: 2020-02-17

CYBER SECURITY ADVISORY

Multiple eSOMS vulnerabilities

ABBVU-PGGA-2018035

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.

Affected Products

eSOMS versions 3.9 to 6.0.3

Vulnerability ID

ABB ID: ABBVU-PGGA-2018035

Summary

An update is available that resolves multiple privately reported vulnerability in the product versions listed above.

In the most severe case, an attacker who successfully exploited these vulnerabilities could take over a user's browser session, discover session based information, or affect the confidentiality of sensitive information within the application.

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.

Additional information can be found in the "Vulnerability Details" section:

CVSS v3				
Vulnerability	**Base Score**	**Temporal Score**	**Vector**	**CVEID**
eSOMS Cache-control (Pragma) HTTP Header	6.5/Medium	5.9/Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	CVE-2019-19000
eSOMS X-Frame-Option	6.5/Medium	5.9/Medium	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	CVE-2019-19001
X-XSS-Protection not enabled	6.3/Medium	5.7/Medium	AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C	CVE-2019-19002
eSOMS: HTTPOnly flag not set	5.3/Medium	4.8/Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	CVE-2019-19003
eSOMS: X-Content-Type-Options Header Missing	6.1/Medium	5.5/Medium	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C	CVE-2019-19089
eSOMS: Secure Flag not set	3.5/Low	3.2/Low	AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	CVE-2019-19090

eSOMS: HTTP response information leakage	4.3/Medium	3.9/Low	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	CVE-2019-19091
eSOMS: Viewstate without MAC Signature	3.5/Low	3.2/Low	AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	CVE-2019-19092
eSOMS: Password complexity issue	6.5/Medium	5.9/Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C	CVE-2019-19093
Vulnerable Redis version	7.3/High	6.6/Medium	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C	
eSOMS: SQL injection vulnerability	7.6/High	6.8/Medium	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C	CVE-2019-19094
eSOMS: Stored XSS vulnerability	5.4/Medium	4.9/Medium	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C	CVE-2019-19095
eSOMS: REDIS clear text credentials	6.1/Medium	5.5/Medium	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C	CVE-2019-19096
eSOMS: SSL medium strength Cipher Suites	5.9/Medium	5.3/Medium	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	CVE-2019-19097

Recommended immediate actions

Some vulnerabilities reported in this advisory are fixed in eSOMS 6.0.3. The remaining are fixed in eSOMS version 6.1. Details of the issues listed below indicate in which version the vulnerability was remediated.

Note: Customers wishing to upgrade to 6.0.3 will still be affected by issues fixed in 6.1.

ABB recommends that customers update their version of eSOMS as soon as possible.

Vulnerability Details

Multiple vulnerabilities exist in the eSOMS web interface that could potentially affect the confidentiality, integrity, or availability of information. The vulnerabilities are described below:

- For ABB eSOMS 4.0 to 6.0.3, The Cache-Control and Pragma HTTP header(s) have not been properly configured within the application response. This can potentially allow browsers and proxies to cache sensitive information. Remediated in eSOMS 6.1
- For ABB eSOMS versions 4.0 to 6.0.2, the X-Frame-Options header is not configured in HTTP response. This can potentially allow 'ClickJacking' attacks where an attacker can frame parts of the application on a malicious web site, revealing sensitive user information such as authentication credentials. Remediated in eSOMS 6.0.3.

- For ABB eSOMS versions 4.0 to 6.0.2, the X-XSS-Protection HTTP response header is not set in responses from the web server. For older web browser not supporting Content Security Policy, this might increase the risk of Cross Site Scripting. Remediated in eSOMS 6.0.3.
- For ABB eSOMS versions 4.0 to 6.0.2, the HTTPOnly flag is not set. This can allow Javascript to access the cookie contents, which in turn might enable Cross Site Scripting. Remediated in eSOMS 6.0.3.
- For ABB eSOMS versions 4.0 to 6.0.3, the X-Content-Type-Options Header is missing in the HTTP response, potentially causing the response body to be interpreted and displayed as different content type other than declared. A possible attack scenario would be unauthorized code execution via text interpreted as JavaScript. Remediated in eSOMS 6.1.
- For ABB eSOMS versions 4.0 to 6.0.2, the Secure Flag is not set in the HTTP response header. Unencrypted connections might access the cookie information, thus making it susceptible to eavesdropping. Remediated in eSOMS 6.0.3.
- For ABB eSOMS versions 4.0 to 6.0.3, HTTPS responses contain comments with sensitive information about the application. An attacker might use this detail information to specifically craft the attack. Remediated in eSOMS 6.1.
- ABB eSOMS versions 4.0 to 6.0.3 use ASP.NET Viewstate without Message Authentication Code (MAC). Alterations to Viewstate might thus not be noticed. Remediated in eSOMS 6.0.3.
- eSOMS versions before 4.0 to 6.0.3 do not enforce password complexity settings, potentially resulting in lower access security due to insecure user passwords. Remediated in eSOMS 6.0.3.
- Vulnerable Redis version. A version of Redis is installed with eSOMS version 6.0 to 6.0.2 that is affected by known vulnerabilities. Remediated in eSOMS 6.0.3.
- Lack of input checks for SQL queries in ABB eSOMS versions 3.9 to 6.0.3 might allow an attacker SQL injection attacks against the backend database. Remediated in eSOMS 6.1.
- Lack of adequate input/output validation for ABB eSOMS versions 4.0 to 6.0.2 might allow an attacker to attack such as stored cross-site scripting by storing malicious content in the database. Remediated in eSOMS 6.0.3.
- The Redis data structure component used in ABB eSOMS versions 6.0 to 6.0.2 stores credentials in clear text. If an attacker has file system access, this can potentially compromise the credentials' confidentiality. Remediated in eSOMS 6.0.3.
- ABB eSOMS versions 4.0 to 6.0.3 accept connections using medium strength ciphers. If a connection is enabled using such a cipher, an attacker might be able to eavesdrop and/or intercept the connection. Remediated in eSOMS 6.1.

Mitigating Factors

In general, recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the organization. Such practices include ensuring process control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that must be evaluated case by case. Process control 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 a control system.

Workarounds

No workarounds have been identified.

Frequently Asked Questions

What is the scope of the vulnerabilities?

In the most severe case, an attacker would be able to obtain information about a user's browsing session or possibly gain unauthorized access to sensitive data from within the application.

What causes the vulnerability?

Many issues result from misconfigured or missing HTTP headers, while other are affected by a lack of proper input sanitization.

What is the affected component?

The eSOMS web application front end, which is used as a web-based client interface to the eSOMS application.

How could an attacker exploit the vulnerability?

An attacker could sniff network traffic in order to discover information about the web session, trick a user into performing a particular action that would reveal information, or gain unauthorized access to data or functionality through the web interface.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system could exploit many of these vulnerabilities.

What does the update do?

The updated versions of eSOMS implement improved input validation and add secure configuration parameters

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.

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.