ADMS netCADOPS Bounds Checking Vulnerability

ABBVU-PGGA-201705

Update Date:

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

3.4, 7.1, 7.2.x, 8.0, and 8.1

Summary

ABB is aware of a reported vulnerability in the netCADOPS web interface that could allow a user to gain information about the server configuration through an error message.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and 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 v2 Base Score: 5.0

CVSS v2 Temporal Score: 3.9

CVSS v2 Vector: *AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C:*

CVSS v2 Link: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

CVSS Base Score: 5.8

CVSS v3 Temporal Score 5.2

CVSS Vector: *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/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:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Corrective Action or Resolution

The following versions are released on their respective branches to address the vulnerability:

ADMS 3.4.34.6

ADMS 7.1.16.1

ADMS 7.2.10

ADMS 8.0.20

ADMS 8.1.7.1

ABB recommends that customers apply the corresponding update as soon as possible.

Vulnerability Details

A vulnerability exists in the netCADOPS web interace where a user who supplies a userid and password greater than 12 characters can generate an error message from the server that contains system configuration information. This information may be able to be used in a more sophisticated attack.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include

that 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 have to 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 workaround has been identified at this time.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this discover system configuration information though an error message.

What causes the vulnerability?
The vulnerability is caused by improper bounds checking for the userid and password field in the netCADOPS web interface.

What is the <affected product or component >?
Affected components include the netCADOPS web interface.

How could an attacker exploit the vulnerability?
An attacker would need to have access to the DMS system and netCADOPS web interface.

Could the vulnerability be exploited remotely?
An attacker would need to have access to the control network hosting DMS.

What does the update do?
The update removes the vulnerability by modifying the way the application validates the userid and password fields.

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.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- Ismail Erkek - Barikat

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

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