Local File Inclusion Vulnerability in FOX515T release 1.0

ABB-VU-PGGA-1KHW028693

Update Date: 2018-01-12

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

FOX515T release 1.0

Vulnerability ID

ABB ID: ABB-VU-PGGA-1KHW028693

Summary

A vulnerability can exist in FOX515T communication equipment. The vulnerability affects the product versions listed above.

The embedded web server deployed in the FOX515T device is vulnerable to Local File Inclusion (LFI) vulnerability. Under certain conditions the web server accepts a parameter that specifies a file for display or for use as a template. The filename provided to the script is not validated by the application, an attacker could retrieve any file on the server.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for CVSS v2. 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:	4.9
CVSS v2 Temporal Score:	4.2
CVSS v2 Vector:	AV:L/AC:L/Au:N/C:C/I:N/A:N/E:F/RL:U/RC:UC
CVSS v2 Link:	http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:L/Au:N/C:C/I:N/A:N/E:F/RL:U/RC:UC)
CVSS v3 Base Score:	7.5
CVSS v3 Temporal Score:	6.8
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:R
CVSS v3 Link:	http://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:R

Corrective Action or Resolution

The product has already been phased out and has reached obsolete status.

The latest release available is R.1.0 ICS10 dated from 12.05.2009. No further maintenance releases are planned.

Vulnerability Details

See summary above.

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.

Industrial 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 are available.

Frequently asked questions

What is the scope of the vulnerability?

Under certain conditions the web server accepts a parameter that specifies a file for display or for use as a template. The filename provided to the script is not validated by the application, so that an attacker could potentially retrieve any file on the server.

When this security advisory was issued, had this vulnerability been publicly disclosed?
This is not known.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?
Yes, ABB had received a report about the existence of the vulnerability.

Acknowledgements

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

- Ketan Bali for reporting this vulnerability

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.