SA-WBM-2018-004: Vulnerabilities in the WAGO e!DISPLAY WBM

Publication Date:	2018-07-10
Last Update:	2018-07-10
Version:	V1.0
Severity:	Important

Description

T. Weber of SEC Consult reported multiple vulnerabilities to the CERT@VDE which impact the security of WAGO e!DISPLAY devices.

Impact

An unauthenticated user can exploit a vulnerability (CVE-2018-12981) to inject code in the WBM via reflected cross-site scripting (XSS), if he is able trick a user to open a special crafted web site. This could allow an attacker to execute code in the context of the user and execute arbitrary commands with restriction to the permissions of the user. Authenticated users can use a vulnerability to inject code in the WBM via persistent cross-site scripting (XSS) via special crafted requests which will be rendered and/or executed in the browser. Authenticated WBM users can transfer arbitrary files to different file system locations (CVE-2018-12980) to which the web server has the required permissions and partially allowing replacing existing files due weak file permissions (CVE-2018-12979) which can result in an authentication bypass.

Affected Products

To our current knowledge following products with FW 01 are affected by these vulnerabilities:

- 762-3000
- 762-3001
- 762-3002
- 762-3003

Vulnerability Characterization

This advisory is based upon the report of SEC Consult.

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)

The vulnerability can be exploited by authenticated and unauthenticated users by sending special crafted requests to the web server allowing injecting code within the WBM. The code will be rendered and/or executed in the browser of the user's browser.

Unrestricted Upload of File with Dangerous Type (CWE-434)

The vulnerability allows an authenticated user to upload arbitrary files to the file system with the permissions of the web server.

Incorrect Permission Assignment for Critical Resource (CWE-732)

Weak permissions allow an authenticated user to overwrite critical files by abusing the unrestricted file upload in the WBM.

Solution

Update your device to the latest firmware (FW 02). In case this is not feasible limit the access to trusted users and devices.

Mitigation

- Update your device to the latest firmware.
- Restrict network access to the device.
- Do not directly connect the device to the internet.
- Restrict the number of users, with access to the device, to a minimum.
- Change the default passwords of devices.
- Do not install software from untrusted sources.
- Do not open web sites or follow links from untrusted sources.

Additional Resources

None

Reported

This vulnerability was originally reported by T. Weber of SEC Consult to CERT@VDE.

Disclaimer

The security instructions given here have exclusively technical-informatory character; contractual stipulations remain unaffected.

http://global.wago.com/en/wago/impressum/software-user-agreement/index.jsp

For updates please visit https://www.wago.com/de/automatisierungstechnik/security regularly, in case of any questions please contact your local sales representative or send your question by email to security@wago.com.