Beckhoff Security Advisory 2023-001:
Open redirect in TwinCAT/BSD package “authelia-bhf”

Publication Date	12/13/2023 (Dec 13th 2023)
This Update	12/13/2023 (Dec 13th 2023)
This Version	1.0
Latest Version	https://download.beckhoff.com/ [...] /advisory-2023-001.pdf
VDE-ID	VDE-2023-067
CVE-ID	CVE-2023-6545
CVSS 3.1	4.3 Medium (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)
Weakness Enumerator	CWE-601 Redirect to Untrusted Site (‘Open Redirect’)

Summary

With TwinCAT/BSD based products the HTTPS request to the Authelia login page accepts user-controlled input that specifies a link to an external site.

Appearance

Component	Included in product	Affected product version (BEFORE and NOT INCLUDING the named version)
authelia-bhf package	TwinCAT/BSD	authelia-bhf package version < 4.37.5

Description

By default TwinCAT/BSD based products have Authelia installed and configured to perform the user authentication for web applications hosted on a target. This installation and configuration is provided with the package named “authelia-bhf”. With the affected versions of the package Authelia is configured to accept user-controlled input via URL parameter that specifies a link which can then be a link to an arbitrary external site.

Please note: The sources for the package “authelia-bhf” are a fork from the original Open Source Software called “Authelia”. The vulnerability was exclusively introduced with that fork and has been removed there. It never became part of “Authelia”.

Mitigation

Use firewall or web-proxy technology at your network perimeter which allow internal clients to access only trusted external sites directly.

Solution

Please update to a recent version of the affected product.

Acknowledgement

Beckhoff Automation thanks Benedikt Kühne, Siemens Energy for reporting the issue and for support and efforts with the coordinated disclosure. Also Beckhoff Automation thanks CERT@VDE for coordination.

Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

Disclaimer

Beckhoff is not responsible for any side effects negatively affecting the real-time capabilities of your TwinCAT control application possibly caused by updates. Beckhoff offers updated images with qualified performance for Beckhoff hardware from time to time. TwinCAT System Manager offers tools which can be of assistance to verify real-time performance after update. A backup should be created every time before installing an update. Only administrators or IT experts should perform the backup and update procedure.

References

[1] Additional information about the latest IPC security advisories is provided here: www.beckhoff.com/secinfo

History

V 1.0	12/13/2023	Publication