PHOENIX CONTACT
INSPIRING INNOVATIONS

Phoenix Contact Inc.
P.O. BOX 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300

Product Change Notification

PCN-AS-9271-2023

Business Unit	Product Line Code	Type of Change	Action	Date of Issue
AS - Automation Systems	DRD	Product Change Notification	Notify Distributors and Field	11/28/2023

The following Phoenix Contact products have been modified. Existing specifications will be met or exceeded. Please review and acknowledge this document and inform your personnel as needed.

Product Change Notification

Description for Product Change Notification

Advisory Title

A Heap-based buffer overflow caused by libcurl, and wrong whitespace character interpretation in Javascript, both used in CodeMeter Runtime are affecting multiple products.

Advisory ID

CVE-2023-38545
CVE-2023-24540
VDE-2023-062

Vulnerability Description

CVE-2023-38545: The affected Wibu-Systems' products internally use the libcurl in a version that is vulnerable to a buffer overflow attack if curl is configured to redirect traffic through a SOCKS5 proxy. A malicious proxy can exploit a bug in the implemented handshake to cause a buffer overflow. If no SOCKS5 proxy has been configured, there is no attack surface

CVE-2023-24540: Not all valid JavaScript whitespace characters are considered to be whitespace. Templates containing whitespace characters outside of the character set "\t\n\f\r\u0020\u2028\u2029" in JavaScript contexts that also contain actions may not be properly sanitized during execution.

Affected Products

Phoenix Contact Activation Wizard <=1.6

Other software listed in the table below

Impact

CVE-2023-38545: In a worst-case scenario and when using a SOCKS5 proxy, a successful exploitation of the vulnerability can lead to arbitrary code execution using the privileges of the user running the affected software .

CVE-2023-24540: WIBU Systems states that WIBU Codemeter is not affected by this vulnerability

Classification of Vulnerability

CVE-2023-38545
Base Score: 9.8
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-787

CVE-2023-24540
Base Score: 9.8
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-74

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

Temporary Fix / Mitigation

Product Change Notification

Disable using a SOCKS5 proxy: □

* The proxy environment variables HTTP_PROXY, HTTPS_PROXY and ALL_PROXY must not be set to socks5h:// □
* Ensure that CodeMeter is not defined to use the SOCKS5 proxy. The variable ProxyServer must not be start with socks5h://.
    - o On Windows, the definition of that variable is in the registry (regedit) under HKLM/SOFTWARE/WIBU SYSTEMS/ CodeMeter/Server/ CurrentVersion
    - o On Mac, the definition of that variable is in the file /Library/ Preferences/com.wibu.CodeMeter.Server.ini
    - o On Linux, the definition of that variable is in the file /etc/wibu/ CodeMeter/Server.ini
    - o On Solaris, the definition of that variable is in the file /etc/opt/ CodeMeter/Server.ini

Use general security best practices to protect systems from local and network attacks like described in the application node AH EN INDUSTRIAL SECURITY

Remediation

PHOENIX CONTACT strongly recommends affected users to upgrade to CodeMeter V7.60d, which fixes these vulnerabilities. WIBU-SYSTEMS has already published an update for CodeMeter on their homepage. Since this current version of CodeMeter V7.60d has not yet been incorporated into Phoenix Contact products, we strongly recommend to download and install the current CodeMeter version directly from the WIBU-SYSTEMS homepage.

Update Phoenix Contact Activation Wizard to version 1.7 when available. Please check the Phoenix Contact e-Shop for related Software updates regularly.

Acknowledgement

Phoenix Contact was informed about these vulnerabilities by WIBU-SYSTEMS. We kindly appreciate the coordinated disclosure of these vulnerabilities by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2023-11-21): Initial publication

Stock Status
Can existing stock still be used?
Is mixture of stock acceptable?

Transaction Dates	
Date modification goes into effect from Germany:	11/28/2023
Expected first shipment (from Phoenix Contact) of the modified products(s):	11/28/2023

Product Change Notification

Should you have any issues with the timeline or content of this product change, please contact Phoenix Contact using the information below. Customers should acknowledge receipt of the PCN within 30 days of delivery of the PCN; provided, however, that the failure to acknowledge receipt does not affect the product change or the effective date thereof.

Contact Info:
Ted Thayer
tthayer@phoenixcontact.com

Thank you,

Zachary Stank

Product Marketing Manager

Product Change Notification

Part #	Type Description
1046008	PLCNEXT ENGINEER
2702889	FL NETWORK MANAGER BASIC
1083065	IOL-CONF