PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

04 March 2019
300439451/imjl01

Security Advisory for Phoenix Contact MEVIEW3

Advisory Title

Vulnerability in WibuKey Network Server Manager

Advisory ID

VDE-2019-003
CVE-2018-3989
CVE-2018-3990
CVE-2018-3991

Vulnerability Description

The latest WibuKey Runtime Version 6.50 of WIBU-SYSTEMS AG fixes the following vulnerabilities:
- CVE-2018-3989
- CVE-2018-3990

Exploiting these vulnerabilities allows unauthorized reading of kernel memory information as well as a potential unauthorized rights extension on the local system.

In addition, the latest WibuKey Runtime version 6.50 fixes the following vulnerability
- CVE-2018-3991

The vulnerability affects all operating systems and allows the potential execution of code on network accessible WibuKey network servers. Only the systems on which a WibuKey network server is running are affected. This applies to systems that provide licenses for an attached WibuBox in the network for use by other clients.

Affected products

WibuKey Network Server is used for licensing visualization systems MEVIEW3. All visualization systems MEVIEW3 with dongle-based licensing are affected.

Impact

CVE-2018-3989:
WIBU-SYSTEMS WibuKey.sys kernel memory information disclosure vulnerability
The vulnerability affects Windows systems and allows unauthorized reading of kernel memory information on the local system.

CVE-2018-3990:
WIBU-SYSTEMS WibuKey.sys pool corruption privilege escalation vulnerability
The vulnerability affects Windows systems and allows potential unauthorized privilege escalation on the local system.

CVE-2018-3991:
WIBU-SYSTEMS WibuKey network server management remote code execution vulnerability
The vulnerability affects all operating systems and allows the potential execution of code on network accessible WibuKey network servers. Only the systems on which a WibuKey network server is running are affected. This applies to systems that provide licenses for an attached WibuBox in the network for use by other clients.

Classification of Vulnerability

CVE-2018-3989:
CVSS V3.0 Base Score: 5.5
CVSS V3.0 Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2018-3990:
CVSS V3.0 Base Score: 7.8
CVSS V3.0 Vector: AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

CVE-2018-3991:
CVSS V3.0 Base Score: 9,8
CVSS V3.0 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Mitigation

a) Dongle-based licensing:
Update WibuKey Runtime to version 6.50.
https://www.wibu.com/support/user/downloads-user-software.html

WibuKey Runtime Version 6.50 will be integrated in the next version MEVIEW3 (3.14.25 & 3.15.18).

b) Hardwarecode-based licensing:

Removing the WibuKey application.

For further information please refer to:

https://www.wibu.com/de/support/anwendersoftware/anwendersoftware/file/download/5638.html

Acknowledgement

PHOENIX CONTACT Energy Automation GmbH was informed about this vulnerabilities by WIBU-SYSTEMS AG