



SPRECON-V460 SECURITY VULNERABILITY ANNOUNCEMENT 2019-01

Vulnerabilities in Wibu Systems WibuKey Software components

Issue 1

CONTENT

CONTENT.....	1
INTRODUCTION.....	3
AFFECTED COMPONENTS.....	3
AFFECTED VERSIONS.....	3
VULNERABILITY DETAILS.....	3
PATCH AVAILABILITY.....	5
KNOWN ISSUES.....	5
MITIGATION.....	5
INSTALLATION, UPDATE.....	5
GENERAL RECOMMENDATIONS.....	6
IMPRINT.....	7

INTRODUCTION

Sprecher Automation informs about three vulnerabilities in the WibuKey software from Wibu Systems.

The WibuKey software is used for dongle licensing by the SPRECON-V460 editor, SPRECON-V460 runtime, SPRECON-V460 web server, SPRECON-V460 logic runtime, straton runtime, SPRECON-V460 logic workbench and the straton workbench, and for some versions is part of the installation of these software products.

SPRECON-V460 versions 8.00 and higher exclusively use the CodeMeter Software from Wibu Systems and are not affected by these vulnerabilities.

The SPRECON-V460 Analyzer exclusively uses the CodeMeter Software from Wibu Systems and is not affected by these issues.

AFFECTED COMPONENTS

- Systems, where the SPRECON-V460 editor, SPRECON-V460 runtime, SPRECON-V460 web server, SPRECON-V460 logic runtime, straton runtime, SPRECON-V460 logic workbench, or straton workbench have been installed, may contain an installation of the WibuKey Runtime software and are potentially affected.
- Systems, where the WibuKey Runtime software has been installed manually, as a WibuKey Network Server for hosting a WibuKey network dongle, are potentially affected.

Systems, that use green WibuKey dongles (centronics parallel interface, USB, other) require the WibuKey Software.

Systems, that use silver CodeMeter dongles, use the CodeMeter Runtime software and do not require the WibuKey Software.

AFFECTED VERSIONS

- WibuKey Software versions 6.40 and older are affected
- SPRECON-V460 products versions 7.20 and older are affected
- SPRECON-V460 products versions 7.50 and 7.60 may be affected if the WibuKey software has been installed manually, to support a WibuKey dongle
- straton products versions 9.2 and older are affected

VULNERABILITY DETAILS

The WibuKey software contains the following three vulnerabilities:

- CVE-2018-3989
- CVE-2018-3990
- CVE-2018-3991

CVE-2018-3989:

WIBU-SYSTEMS WibuKey.sys kernel memory information disclosure vulnerability

CVSS v3 base score and vector:

A CVSS base score of 4.3 has been calculated for this vulnerability.

The corresponding CVSS v3 vector: [AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N](#)

Additional information:

The vulnerability is present on all systems with a vulnerable version of the WibuKey Runtime installed.

Mitigations:

No mitigation options are known. Only an update of the WibuKey Runtime Software, or removing the WibuKey Runtime Software, can resolve this vulnerability.

CVE-2018-3990:

WIBU-SYSTEMS WibuKey.sys pool corruption privilege escalation vulnerability

CVSS v3 base score and vector:

A CVSS base score of 9.3 has been calculated for this vulnerability.

The corresponding CVSS v3 vector: [AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H](#)

Additional information:

The vulnerability is present on all systems with a vulnerable version of the WibuKey Runtime installed.

Mitigations:

No mitigation options are known. Only an update of the WibuKey Runtime Software, or removing the WibuKey Runtime Software, can resolve this vulnerability.

CVE-2018-3991:

WIBU-SYSTEMS WibuKey network server management remote code execution

CVSS v3 base score and vector:

A CVSS base score of 10.0 has been calculated for this vulnerability.

The corresponding CVSS v3 vector: [AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H](#)

Additional information:

This vulnerability exists only when the WibuKey software was installed manually and the option to install the WibuKey WkNet / WkLAN Server and run the WibuKey WkNet / WkLAN Server as a Windows Service were explicitly enabled during installation. In this case, the WibuKey WkNet / WkLAN Server, by default, is listening on TCP port 22347.

When the WibuKey Runtime Software is automatically installed, in combination with a SPRECON-V460 version, this option is not enabled and the WibuKey WkNET / WkLAN server is not installed as a Windows Service.

Mitigations:

No mitigation options are known. Only an update of the WibuKey Runtime Software, or removing the WibuKey Runtime Software, can resolve this vulnerability, when the WibuKey Dongle is required to be available as a Network Dongle.

PATCH AVAILABILITY

Wibu Systems provides an updated version 6.50 of the WibuKey software that addresses the reported vulnerabilities. The “WibuKey Runtime for Windows” software version 6.50 can be downloaded following this link: <https://www.wibu.com/support/user/downloads-user-software.html>

KNOWN ISSUES

The version 6.50 build 3307 of the WibuKey Runtime for Windows software has a known issue with parallel WibuKey dongles. On start-up of the SPRECON-V460 editor or the SPRECON-V460 runtime, an error message appears stating “Licensing failed: Function = WkbSelect2() The specified parameter is invalid (4)”. Acknowledging the error allows a normal start of the application with the license intact.

MITIGATION

With versions SPRECON-V460 7.20 and older, the WibuKey Runtime software is installed automatically by the setup procedure, in order to be able to use WibuKey dongles without requiring a manual installation of this software.

When the installed product uses either a CodeMeter Dongle or a soft license, the WibuKey Runtime software is not needed and can be uninstalled through the Windows control panel. Uninstalling the WibuKey Runtime software removes the vulnerabilities.

With versions SPRECON-V460 7.50 and 7.60, the WibuKey Runtime software is no longer installed automatically as part of the setup procedure but is delivered together with the installation media. It is therefore possible, that the WibuKey Runtime software has been installed manually at some point but may not, or may no longer, be needed.

INSTALLATION, UPDATE

The installer of the WibuKey Runtime for Windows software is capable of updating an existing installation. It is not required to uninstall the existing WibuKey Runtime for Windows software first. It is recommended to close all applications during the installation of the updated WibuKey Runtime for Windows software.

It is recommended to unplug WibuKey USB dongles prior to installing the updated WibuKey Runtime for Windows software.

In most cases, the installation will require a restart of the system for the update to be completed successfully. A restart of the system, even if not prompted, is recommended.

When the WibuKey that is used is a local dongle (most likely scenario) and not a network dongle, the option to install the WibuKey Server is not required. In this case, disable the checkbox “32 bit WkNet/WkLAN Network server” when installing the update.

The WibuKey Runtime software version 6.50 is compatible with current Windows versions and previous Windows versions, including Windows XP.

GENERAL RECOMMENDATIONS

Sprecher Automation generally recommends restricting local physical access to authorized people only. Network access shall be limit to communication that is absolutely required.

Using VLANs and firewalls to segment network traffic and create zones and conduits, reduces exposure of vulnerable systems and allows access to a WibuKey WKLAN Server to be restricted to only those systems that are in fact using a network dongle.

Sprecher Automation further recommends using application whitelisting to restrict execution of applications to only those applications that are required for the operation of the system.

IMPRINT

Sprecher Automation GmbH
Franckstrasse 51, 4020 Linz, Austria
T: +43 732 6908-0, F: +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.at

© 2019 Sprecher Automation GmbH
Alle Rechte vorbehalten / All rights reserved.

Distribution and/or reproduction of this document or parts thereof in any form is permitted solely with the written permission of Sprecher Automation GmbH. The technical data contained herein have been provided solely for informational purposes and are not legally binding. Subject to change, technical or otherwise.