Security Vulnerability Announcement 2019_1

Vulnerabilities in Wibu Systems WibuKey Software components

www.copadata.com
sales@copadata.com

zenon
by COPA-DATA

1. History

Date	Comment
07.12.2018	Created
21.12.2018	Updated
08.01.2019	Updated with TCP port information for WkLAN
21.01.2019	Updated with version 6.50a build 3320
23.01.2019	Updated with note regarding existing zenon installations and removing zenon and installing zenon
28.01.2019	Updated with availability of updated .ISO and .BIN files on the website
28.02.2019	Updated to new design

Content

2. Introduction

COPA-DATA has received a report from Wibu Systems, detailing three severe security vulnerabilities in the WibuKey Runtime software.

The WibuKey Runtime software is used for dongle licensing by the zenon editor, zenon runtime, zenon web server, zenon logic runtime and the straton workbench. For some versions, this software is part of the installation of these software products, even if no dongle license is being used.

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

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

On December 20th 2018, the information on these vulnerabilities was publically available through the Cisco Talos security website for two days until it was removed again pending the official disclosure date. By the time the information was removed, it was already referenced and taken over by other sources.

3. Products affected

Systems where the zenon editor, zenon runtime, zenon web server, zenon 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 Runtime software.

Systems that use silver CodeMeter dongles, use the CodeMeter Runtime software and do not require the WibuKey Runtime software. On such systems the WibuKey Runtime software may still be installed.

Note: The WibuKey Runtime software and / or WibuKey Dongles may also be used by software products from other vendors.

4. Versions affected

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

5. Vulnerability details

The report by Wibu Systems contains the following three vulnerabilities. Details are provided for each vulnerability individually.

- 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 Runtime 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 zenon 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, can resolve this vulnerability, when the WibuKey Dongle is required to be available as a Network Dongle. When the WibuKey Runtime is not required to be available as a Network Dongle, the WibuKey Runtime software may be removed or reconfigured to not allow network access.

6. Patch Availability

Wibu Systems provides an updated version 6.50a – build 3320 of the WibuKey Runtime software that addresses the reported vulnerabilities.

Earlier in December 2018, Wibu Systems provided an updated version 6.50 of the WibuKey software that also addresses the reported vulnerabilities but contains interoperability issues with COPA-DATA products and parallel dongles.

The “WibuKey Runtime for Windows” software version 6.50a can be downloaded following this link:

https://www.wibu.com/support/user/downloads-user-software.html

7. Known issues

The version 6.50 build 3307 of the WibuKey Runtime for Windows software has a known issue with parallel WibuKey dongles. On startup of the zenon editor or the zenon 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. This issue is resolved with WibuKey Runtime for Windows version 6.50a.

8. Mitigation

With versions zenon 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.

When the installed product uses a WibuKey Dongle, uninstalling the WibuKey Runtime software removes the vulnerabilities but also fails to start the product with a valid Dongle License. In this case there is no mitigation and the updated version must be installed.

With versions zenon 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.

9. Update

Recommendations

COPA-DATA recommends that system integrators and asset owners perform a risk assessment to establish whether the updated version of the WibuKey Runtime software shall be installed.

Considering the criticality of the issues reported, COPA-DATA follows the advice of Wibu Systems, and recommends installing the update at the earliest opportunity.

COPA-DATA recommends testing the updated version of the WibuKey software in a test environment to verify normal operation of the system according to project specific configuration and hardware environment, prior to installing the patch in a production environment.

COPA-DATA recommends that a contingency plan is in place to roll back the installation of the patch in case of any unexpected issues with the production environment following the installation of the patch.

Procedure

For existing installations using a WibuKey Dongle, it is necessary to download the updated WibuKey Runtime for Windows version 6.50a from Wibu Systems and install this version on the affected systems in order to resolve the security vulnerabilities. (See Patch Availability for the link)

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.

Close all applications during the installation of the updated WibuKey Runtime for Windows software.

Unplug WibuKey USB dongles prior to installing the updated WibuKey Runtime for Windows software.

During the installation the setup may ask to reset settings to their respective default. If the WibuKey Runtime software is configured to use a Network Dongle, confirming the reset of the settings to the default, removes the configured Network Dongle. It is recommended to not overwrite the settings in this case.

Perform a restart of the system for the update to be completed successfully, if prompted. A restart of the system, even if not prompted, is recommended.

When the WibuKey is used as a local dongle (most likely scenario) and not as 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 6.50a is compatible with current Windows versions and previous Windows versions, including Windows XP.

10. Installation Media

For versions zenon 7.00 and newer, COPA-DATA provides updated versions of the .ISO and .BIN downloads on the COPA-DATA website that include the updated version 6.50a of the WibuKey Runtime software. These .ISO and .BIN files can be used for new installations.

COPA-DATA provides an up-to-date version of the USB drives with new licenses that include the updated version 6.50 of the WibuKey software, for versions 7.00 and newer.

Updated installation media version 7.00:

For this zenon version, the WibuKey Runtime Software installed by the setup is the old version containing the vulnerabilities. The updated WibuKey Runtime version 6.50a, addressing the vulnerabilities, is included in the folder “.\Additional_Software\Wibu Key Dongle Software x86” and “.\Additional_Software\Wibu Key Dongle Software x64”. The updated WibuKey Runtime version 6.50 needs to be installed manually, following the completion of the setup.

Updated installation media version 7.10, version 7.11 and version 7.20:

For these versions, the WibuKey Runtime Software installed by the setup is the updated WibuKey Runtime version 6.50a that addresses the vulnerabilities. Additionally the folders “.\AdditionalSoftware\WibuKey” for 7.10 and 7.11 and “.\AdditionalSoftware\WIBU-SYSTEMS WibuKey” for 7.20, contain either the updated WibuKey Runtime version 6.50a or a batch file that installs this version.

Note regarding existing installations:

While installation media for versions 7.10, 7.11 and 7.20 contain an updated version of the WibuKey Runtime software, the current version of the WibuKey Runtime software is only installed when no previous WibuKey Runtime Software exists on the system.

Uninstalling zenon and installing zenon again using the updated installation media, will not result in an updated WibuKey Runtime Software. In this case, either uninstall WibuKey Runtime Software explicitly after uninstalling zenon, or manually install the WibuKey Runtime Software version 6.50a.

Updated installation media version 7.50 and version 7.60:

For these versions, the WibuKey Runtime Software is generally not installed automatically by the setup. The folder ".\AdditionalSoftware\WIBU-SYSTEMS WibuKey" contains the updated WibuKey Runtime Software version 6.50a.

Please contact your COPA-DATA representative if you have any questions on updating or replacing your existing installation media.

11. General recommendations

COPA-DATA 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. It is recommended that systems hosting a WibuKey WkLAN Server are not facing external networks.

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

12. Acknowledgements

COPA-DATA wishes to thank Wibu Systems for announcing the publication of these issues to their partners, prior to the public release.