electrocon
international incorporated

405 Little Lake Dr., Suite C
Ann Arbor, Michigan 48103

Tel: (734) 761-8612
Fax: (734) 761-8078
Email: eii@electrocon.com
Web: www.electrocon.com

September 15, 2017

Subj: Corrected Security Vulnerability in Wibu-Systems' CodeMeter Software: Explanation and What You Should Do

To Our CAPE Users and Evaluators:

Yesterday we became aware of the discovery of a potential security flaw in the Wibu-Systems' CodeMeter runtime software that we distribute with most copies of our CAPE 14 software. This software supports the hardware license protection keys ("dongles") needed to run CAPE. If your version of CAPE requires a hardware key to run, or if you are using a demonstration copy of CAPE, this notice applies to you.

The security vulnerability was discovered by a friendly entity, is rated as being of Medium severity, and has not been exploited to our knowledge.

Wibu-Systems has eliminated the security vulnerability in the latest version of its CodeMeter Runtime software, version 6.50c.

The recommended action is simply to update the CodeMeter software on each machine that runs CAPE. The method is described below under "Recommended Action." Your action is important but not urgent.

Except for the Recommended Action section below, the remainder of this letter contains detail that most likely will be of interest only to your Information Technology people. So, please share this notice with them.

Recommended Action:

Users running CodeMeter Runtime versions prior to 6.50b should install the CodeMeter Runtime 6.50c as soon as possible. To upgrade the CodeMeter Runtime, download and install version 6.50c. It is not necessary to remove the prior version; it will be upgraded in place. The CodeMeter Runtime 6.50c is available directly from Wibu-Systems at:

https://www.wibu.com/downloads-user-software/file/download/4437.html

or from Electrocon at:

https://electrocon.com/files/CodeMeterRuntime_v6.50c.exe

Please contact Electrocon with any questions or concerns. Technical details on the vulnerability are available from the references below.

We certainly apologize for the inconvenience this may cause you. However, events like this seem to be an unavoidable, and definitely unwelcome, component of the Information Age in which we live.

Sincerely,

Paul F. McGuire
President

To the Information Technology Personnel Who Support Our CAPE Users:

Title: Electrocon Third Party Component: Wibu-Systems' CodeMeter Runtime – Persistent XSS Vulnerability

CVE-ID: CVE-2017-13754

Date: 2017-09-15

Severity: CVSSv3 Base Score: 5.4 (Medium) (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N)

Summary:

CAPE 14 demonstration software and CAPE 14 software with hardware keys includes the CodeMeter Runtime, a component from Electrocon's third party vendor, Wibu-Systems. This service is used for management of your CAPE 14 license. Wibu-Systems has identified a persistent XSS vulnerability in the CodeMeter Runtime WebAdmin component for all versions prior to v6.50b. Electrocon is issuing this security advisory to alert customers who use this component.

Versions Affected:

CodeMeter Runtime before 6.50b, distributed with CAPE 14 and earlier versions that require activation or hardware keys dated September 14, 2017 and earlier.

Versions Unaffected:

CodeMeter Runtime 6.50b and later, distributed with CAPE 14 versions that require activation or hardware keys dated September 15, 2017 and later.

Versions of CAPE 14 that do not say "Software Activation Required" or "Hardware Key Required" on the original disc do not include the vulnerable component.

Recommended Action:

Users running CodeMeter Runtime versions prior to 6.50b should install the CodeMeter Runtime 6.50c as soon as possible. To upgrade the CodeMeter Runtime, download and install version 6.50c. It is not necessary to remove the prior version; it will be upgraded in place. The CodeMeter Runtime 6.50c is available directly from Wibu-Systems at:

https://www.wibu.com/downloads-user-software/file/download/4437.html

or from Electrocon at:

https://electrocon.com/files/CodeMeterRuntime_v6.50c.exe

Please contact Electrocon with any questions or concerns. Technical details on the vulnerability are available from the references below.

References:

https://www.vulnerability-lab.com/get_content.php?id=2074

https://nvd.nist.gov/vuln/detail/CVE-2017-13754