ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-098-01 CANARY LABS, INC. TRENDLINK INSECURE ACTIVEX CONTROL METHOD

April 08, 2013

OVERVIEW

This advisory provides mitigation details for a vulnerability in the Canary Labs, Inc. TrendLink software.

Researcher Kuang-Chun Hung of Security Research and Service Institute−Information and Communication Security Technology Center (ICST) has identified an insecure ActiveX control method vulnerability in Canary Labs, Inc. TrendLink ActiveX control. Canary Labs, Inc. has updated TrendLink, and Kuang-Chun Hung has tested the patch and verified that it mitigates the vulnerability. If exploited, an attacker could influence the paths or file names that are used in the software application. This could affect systems using TrendLink in the critical manufacturing and energy sectors in the United States, South America, and Europe.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

Canary Lab, Inc. reports that the vulnerabilities affect the following products:

- TrendLink Versions 9.0.2.27051 and prior.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IMPACT

Successful exploit of this vulnerability could result in a denial of service (DoS) or remote code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Canary Labs, Inc. is a US-based company that has products deployed in 24 countries, including the United States, South America, and Europe.

The affected product, TrendLink,[a] is a trending application that can be used in SCADA systems. According to Canary Labs, Inc., these products are deployed across several sectors including the critical manufacturing and energy sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSECURE ACTIVEX CONTROL METHOD[b]

TrendLink uses an ActiveX control that contains an insecure ActiveX control method. This control is loaded from "TrendDisplay.dll," and contains a method called "SaveToFile" that allows users to save arbitrary files to any location on the server hosting the control. This vulnerability could result in a DoS or allow remote code execution.

CVE-2012-3022[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.9 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:S/C:N/I:C/A:C).[d]

a. Canary Labs, Inc. TrendLink, http://www.canarylabs.com/software/canary-trend-link, Web site last accessed April 08, 2013.
b. CWE-73: External Control of File Name or Path, http://cwe.mitre.org/data/definitions/73.html, Web site last accessed April 08, 2013.
c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3022, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:S/C:N/I:C/A:C), Web site last accessed April 08, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with medium skill could exploit this vulnerability.

MITIGATION

Canary Labs, Inc. has published a customer notification concerning this vulnerability. TrendLink customers who wish to obtain the update and instructions on how to apply it should contact Canary Labs product support:

> Canary Labs Product Support[e]
> 814-793-3770
> support@canarylabs.com

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth

e. Canary Labs Product Support, http://www.canarylabs.com/services-and-support/product-support, Web site last accessed April 08, 2013.

Strategies.[f] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies,[g] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed April 08, 2013.
g. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed April 08, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

I see that this document is labeled as TLP = WHITE. May I distribute this to other people? According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[h,i] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.

TLP = WHITE: Unlimited

h. Traffic Light Protocol—International CIIP Directory, Issue 21, September 2009.

i. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed April 08, 2013.