ICS-CERT ADVISORY

ICSA-12-265-01—EMERSON DELTAV BUFFER OVERFLOW

September 28, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-12-265-01P on the US-CERT Portal on September 21, 2012. This web page release was delayed to provide the vendor time to contact customers concerning this information.

Researcher Kuang-Chun Hung of the Security Research and Service Institute-Information and Communication Security Technology Center (ICST) has identified a buffer-overflow vulnerability in the Emerson DeltaV application.

This vulnerability can be exploited by a remote attacker; however, no publicly available exploits are currently known to exist. Emerson has produced a hotfix that mitigates this vulnerability. ICST has tested this hotfix and confirms that it fully resolves the vulnerability.

AFFECTED PRODUCTS

The following supported Emerson products are affected:

- DeltaV V9.3.1, V10.3.1, V11.3, and V11.3.1

IMPACT

This vulnerability, if exploited, could allow denial of service.

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

Emerson is a global manufacturing and technology company offering multiple products and services in the industrial, commercial, and consumer markets through its network power, process management, industrial automation, climate technologies, and tools and storage businesses.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW[a]

The DeltaV service allows a string to be copied without bounds checking. By sending a large string to a specific port, an attacker could cause a crash.

CVE-2012-3035[b] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C: N/I:N/A:P).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Emerson has created a hotfix that resolves this vulnerability.

Emerson has distributed a notification in KBA NK-1200-0170 to customers who own a DeltaV Control System; the notification provides details of the vulnerability, recommended mitigations, and instructions on obtaining and installing the hotfix. Customers using DeltaV V9.3.1 and V10.3 are recommended to update to V10.3.1 as there is no hotfix for those versions.

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

---

a. CWE-120: Buffer Copy without Checking Size of Input, http://cwe.mitre.org/data/definitions/120.html, Web site last accessed September 27, 2012.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3035, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:P), Web site last accessed September 27, 2012.

- 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 Strategies.[d] 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-12-146-01A—Cyber Intrusion Mitigation Strategies,[e] 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 industrial control systems security 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/.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 27, 2012.

e. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 27, 2012.

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.