ICS-CERT ADVISORY

ICSA-12-138-01—EMERSON DELTAV MULTIPLE VULNERABILITIES

May 30, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-12-138-01P to the US-CERT secure portal on May 17, 2012, and released Update A on May 21, 2012. This web page release (including Update A) was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of the Security Research and Service Institute—Information and Communication Security Technology Center (ICST) has identified multiple vulnerabilities in the Emerson DeltaV application.

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

AFFECTED PRODUCTS

The following Emerson products are affected:

- DeltaV and DeltaV Workstations,
- V9.3.1, V10.3.1, V11.3, and V11.3.1,
- DeltaV ProEssentials Scientific Graph, and
- V5.0.0.6

IMPACT

These vulnerabilities, if exploited, could allow denial of service, information disclosure, 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 these vulnerabilities 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

CROSS-SITE SCRIPTING[a]

This vulnerability enables an attacker to inject client side script into web pages viewed by other users or bypass client side security mechanisms imposed by modern web browsers. If successfully exploited, this vulnerability could allow arbitrary code execution and may require social engineering to exploit.

CVE-2012-1814[b] has been assigned to this vulnerability. A CVSS V2 base score of 7.5 has also been assigned.

SQL INJECTION[c]

This vulnerability can be used by an attacker to perform database operations that were unintended by the web application designer and, in some instances, can lead to total compromise of the database server. This vulnerability, if successfully exploited, could allow arbitrary code execution.

CVE-2012-1815[d] has been assigned to this vulnerability. A CVSS V2 base score of 7.5 has also been assigned.

a. http://cwe.mitre.org/data/definitions/79.html, Web site last accessed May 30, 2012.
b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1814, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
c. http://cwe.mitre.org/data/definitions/89.html, Web site last accessed May 30, 2012.
d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1815, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

DENIAL OF SERVICE[e]

A denial of service can be created by sending a specially crafted packet to PORTSERV.exe on both TCP/111 and UDP/111. This attack will cause the software to crash, denying service to legitimate users.

CVE-2012-1816[f] has been assigned to this vulnerability. A CVSS V2 base score of 5 has also been assigned.

BUFFER OVERFLOW[g]

In the affected version, DeltaV does not properly sanitize the inputs from project files. Invalid information in certain fields can cause the program to crash and could be used to execute arbitrary code.

CVE-2012-1817[h] has been assigned to this vulnerability. A CVSS V2 base score of 4.6 has also been assigned.

FILE MANIPULATION[i]

If successfully exploited, an attacker can overwrite arbitrary files on the victim's computer in the context of the vulnerable application using the ActiveX control.

CVE-2012-1818[j] has been assigned to this vulnerability. A CVSS V2 base score of 7.5 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

e. http://cwe.mitre.org/data/definitions/400.html, Web site last accessed May 30, 2012.
f. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1816, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
g. http://cwe.mitre.org/data/definitions/119.html, Web site last accessed May 30, 2012.
h. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1817, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
i. http://cwe.mitre.org/data/definitions/618.html, Web site last accessed May 30, 2012.
j. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1818, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a medium skill level would be able to exploit these vulnerabilities.

MITIGATION

Emerson has created a hotfix that resolves these vulnerabilities.

Emerson has distributed a notification in KBA NK-1200-0091 ICS-CERT ADVISORY—ICSA-12-137-01 Emerson Multiple Vulnerabilities: Impact and Recommended Actions to customers who own a DeltaV Control System; the notification provides details of the vulnerabilities, recommended mitigations, and instructions on obtaining and installing the hotfix.

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.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[k] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in email messages.

k. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html Web site last accessed May 30, 2012.

2. Refer to Recognizing and Avoiding Email Scams[l] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[m] for more information on social engineering attacks.

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

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.

l. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, last accessed May 30, 2012.
m. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, last accessed May 30, 2012.