ICS-CERT ADVISORY

ICSA-12-271-01—C3-ILEX EOSCADA MULTIPLE VULNERABILITIES

November 01, 2012

OVERVIEW

This Advisory is a follow-up release to the original Advisory which was posted to the US-CERT secure Portal library October 08, 2012.

Dale Peterson of Digital Bond has identified multiple vulnerabilities in the C3-ilex's EOScada application that can result in data leakage and a denial-of-service (DoS) condition. C3-ilex's has produced a patch that resolves these vulnerabilities.

AFFECTED PRODUCTS

C3-ilex reports that the vulnerabilities affect all EOScada versions prior to 11.0.19.2.

IMPACT

Successful exploitation of these vulnerabilities may cause a DoS or data leakage.

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

C3-ilex's EOScada is a real-time Windows-based Energy Management System for electrical, water, sewage, and gas applications. The EOScada platform features a distributed processing, networked configuration using PCs running Microsoft Windows. The EOScada product line includes PC-based Master Stations as well as remote terminal units (RTUs) that perform communication, data concentration, and connections to a variety of intelligent electronic devices (IEDs).

EOScada is used primarily in the electrical sector with some usage in the water and oil and natural gas sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER ACCESS CONTROL[a]

The EOS Core Scada.exe does not restrict access that causes a DoS condition when attached to Port 5050/TCP or Port 24004/TCP, and any random data are sent to either port. The application will crash and restart and will be unavailable to legitimate users during that time.

CVE-2012-1810[b] has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:P).[c]

RESOURCE MANAGEMENT ERRORS[d]

The EOSDataServer.exe attached to Port 24006/TCP is susceptible to a Resource Management Error when a large amount of random data is sent to the port.

CVE-2012-1811[e] has been assigned to this vulnerability. A CVSS V2 base score of 7.8 has also been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[f]

DATA LEAKAGE[g]

The eosfailoverservice.exe returns data in clear text when a connection is made to Port TCP/12000.

a.http://cwe.mitre.org/data/definitions/284.html, Web site last accessed November 01, 2012.
b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1810. 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 November 01, 2012.
d. http://cwe.mitre.org/data/definitions/399.html, Web site last accessed November 01, 2012.
e. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1811. NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last accessed November 01, 2012.
g. http://cwe.mitre.org/data/definitions/200.html , Web site last accessed November 01, 2012.

CVE-2012-1812[h] has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:N).[i]

RESOURCE MANAGEMENT ERRORS[j]

The eosfailoverservice.exe attached to Port 12000/TCP is susceptible to a Resource Management Error when a large amount of random data is sent to the port.

CVE-2012-1813[k] has been assigned to this vulnerability. A CVSS V2 base score of 7.8 has also been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C). [l]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

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

MITIGATION

C3-ilex recommends customers install the EOScada patch. Customers with a service agreement should contact C3-ilex's Helpdesk at helpdesk@c3ilex.com or by calling the Help Desk at (510) 659-8300 x 107 for instructions on how to obtain the release. Customers without a service agreement should contact their C3-ilex Sales Manager for assistance in purchasing this or a later version release.

h. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1812. NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
i. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:P/A:N), Web site last accessed November 01, 2012.
j. http://cwe.mitre.org/data/definitions/399.html, Web site last accessed November 01, 2012.
k. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1813. NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
l. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last accessed November 01, 2012.

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, specifically addressing traffic to the ports listed above, 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 US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[m] 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.

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/.

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.

m. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed November 01, 2012.

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.