ICS-CERT ADVISORY

ICSA-12-102-01—CERTEC WEBMI2ADS MULTIPLE VULNERABILITIES

April 11, 2012

OVERVIEW

ICS-CERT released an alert titled "ICS-ALERT-11-283-02 – Certec atvise webMI Multiple Vulnerabilities"[a] to the ICS-CERT web page on October 10, 2011.

Independent researcher Luigi Auriemma has identified multiple vulnerabilities in Certec's webMI2ADS application. These vulnerabilities and proof of concept code were disclosed without coordination with ICS-CERT, the vendor, or any other coordinating entity. Certec has produced an update that resolves these vulnerabilities. Mr. Auriemma has verified that the update resolves the identified vulnerabilities.

AFFECTED PRODUCTS

Certec webMI2ADS – All versions prior to Version 2.0.2 are affected.

IMPACT

Successful exploitation of these vulnerabilities may allow an attacker to cause a denial of service (DoS) or could lead to 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

Certec EDV GmbH is an Austrian-based company with regional partners in Germany, Switzerland, Italy, and Israel.

Certec webMI2ADS is the server component of a browser-based HMI system. WebMI2ADS is used primarily in factory and building automation.

a. http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-283-02.pdf, website last accessed April 10, 2012

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DIRECTORY TRAVERSAL[b]

The web server in webMI does not implement sufficient measurers to prevent reading files from an unauthorized directory. An attacker could exploit this vulnerability by sending a specially crafted request to the web server on Port 80/TCP. A successful attack may result in data leakage.

CVE-2011-4880[c] has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned.

NULL POINTER[d]

The web server in webMI does not implement checks on a return value from a function . An attacker could exploit this vulnerability by sending a specially crafted request to the web server on Port 80/TCP. A successful attack would result in a DoS condition.

CVE-2011-4881[e] has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned.

TERMINATION OF THE SOFTWARE[f]

An attacker could use a non-authenticated command via the web interface on Port 80/TCP to shut down the application. A successful attack would result in a DoS condition.

CVE-2011-4882[g] has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned.

RESOURCES CONSUMPTION[h]

The web server in webMI does not implement checks for invalid values in an HTTP request. An attacker could exploit this vulnerability by sending a specially crafted request to the web server on Port 80/TCP. Successful attack would result in a DoS condition.

b. http://cwe.mitre.org/data/definitions/22.html, website last accessed April 10, 2012.
c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4880, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
d. http://cwe.mitre.org/data/definitions/476.html, website last accessed April 10, 2012.
e. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4881, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
f. http://cwe.mitre.org/data/definitions/732.html, website last accessed April 10, 2012.
g. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4882, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
h. http://cwe.mitre.org/data/definitions/400.html, website last accessed April 10, 2012.

CVE-2011-4883[i] has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level may cause a DoS condition or access sensitive data.

MITIGATION

Certec has released version 2.0.2 of webMI2ADS which fixes these vulnerabilities. Customers can download version 2.0.2 of webMI2ADS at: http://www.atvise.com/en/atvise-downloads/products

Users will need to be registered in order to download the new product.

Certec and ICS-CERT recommend that owners of vulnerable versions of the webMI2ADS product download and install the updated version as soon as possible.

ICS-CERT also 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*

i. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4883, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

Strategies.[j] 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:

E-mail: 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.

j. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 10, 2012.