ICS-CERT ADVISORY

ICSA-12-262-01—FULTEK WINTR DIRECTORY TRAVERSAL

September 18, 2012

OVERVIEW

Researcher Daiki Fukumori of Cyber Defense Institute[a] has identified a directory traversal vulnerability in Fultek's WinTr Scada application. Fultek was unable to validate this vulnerability and has not offered any mitigation plans.

ICS-CERT has validated the vulnerability. This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following product is affected:

- WinTr Scada 4.0.5 and earlier.

IMPACT

Successful exploitation of this vulnerability may result in information leakage.

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

Fultek is a company based in Turkey. The affected product, WinTr Scada, is a Web-based SCADA system.

a. Cyber Defense Institute, http://www.cyberdefense.jp/en/, Web site last accessed September 18, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

RELATIVE PATH TRAVERSAL[b]

The WinTr Web server does not sanitize user input. By sending a specially crafted request to the Web server, an attacker may retrieve arbitrary files.

CVE-2012-3011[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:N/A:N).[d]

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

The vendor has not offered any mitigation plans.

According to MITRE, the best mitigation for this type of vulnerability is to properly sanitize user input. MITRE also recommends, when the application is controlled by a third party and the code cannot be fixed, an application firewall may be used to validate input and mitigate the

b. CWE, http://cwe.mitre.org/data/definitions/23.html, CWE-23: Relative Path Traversal, Web site last accessed September 18, 2012.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3011, 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:L/Au:N/C:C/I:N/A:N), Web site last visited September 18, 2012.

vulnerability. Running the application in a sandbox environment may also limit the scope of a compromise.[e]

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 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-12-146-01A—Cyber Intrusion 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 industrial control systems security information and incident reporting: www.ics-cert.org

e. CWE, http://cwe.mitre.org/data/definitions/22.html, CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Web site last accessed September 18, 2012.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 18, 2012.

g. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 18, 2012.

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.