ICS-CERT ADVISORY

ICSA-12-214-01—SIEMENS SYNCO OZW DEFAULT PASSWORD

August 01, 2012

OVERVIEW

Siemens has reported to ICS-CERT that a default password vulnerability exists in the Siemens Synco OZW Web Server device used for building automation systems. Siemens urges their customers to set a secure password on their device's web interface. This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that the default password vulnerability affects the following Synco models:

- OZW775
- OZW672.01, OZW672.04, OZW672.16
- OZW772.01, OZW772.04, OZW772.16, OZW772.250.

For the listed products, all firmware versions prior to Version 4 do not force users to change their password on initial login.

IMPACT

An attacker could use the default password in these devices to gain unauthorized administrative access to the building automation network.

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

Siemens Synco OZW devices are used for remote operation and monitoring of building automation devices. The affected models offer interfaces that can be used over networks, such as the Internet.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DEFAULT PASSWORD[a]

Siemens Synco OZW devices are shipped with a default password protecting administrative functions. The installation procedure does not enforce a password change. This leaves a potential security gap in the asset owner/operator's network.

CVE-2012-3020[b] has been assigned to this vulnerability. A CVSS v2 base score of 9.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:C).[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 level could exploit these vulnerabilities.

MITIGATION

Siemens has released a firmware update (Version 4) and security advisory (SSA-283911)[d] for the OZW672 and OZW772 devices that enforces a password change at initial login.[e] Customers may upgrade to

a. CWE-262: Not Using Password Aging, http://cwe.mitre.org/data/definitions/262.html, Web site last accessed August 13, 2012.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3020, 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:A/AC:L/Au:S/C:C/I:C/A:C), Web site last accessed August 13, 2012.

[d] Siemens security advisory, http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Web site last accessed August 13, 2012

e Siemens password change at initial login, http://support.automation.siemens.com/WW/view/en/41929231/130000, Web site last accessed August 13, 2012

this firmware version, but this is not required to change the default password on existing devices. Siemens urges customers to set a secure password on the web interface for all network devices.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks by performing the following tasks:

- 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), recognize 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.[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-12-146-01—Cyber Intrusion Mitigation Strategies,[g] which 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 CSSP Information and Incident Reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 13, 2012.

g. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed August 13, 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.