ICS-CERT ADVISORY

ICSA-11-167-01—HEAP OVERFLOW VULNERABILITIES IN SUNWAY FORCECONTROL AND PNETPOWER

June 16, 2011

OVERVIEW

ICS-CERT has received a report from Security researcher Dillon Beresford of NSS Labs[a] concerning vulnerabililities affecting Sunway ForceControl and pNetPower SCADA/HMI applications. The reported vulnerabilities are heap-based buffer overflows[b] that could result in a denial of service or the execution of arbitrary code.

ICS-CERT has coordinated with the researcher, China National Vulnerability Database (CNVD), and Sunway to ensure full remediation of the reported vulnerabilities. Sunway has issued two patches that address both vulnerabilities. CNVD has confirmed the effectiveness of the patches issued by Sunway. Neither ICS-CERT nor the researcher has validated these patches. Sunway has issued a security bulletin describing their response.[c]

AFFECTED PRODUCTS

According to the researcher, these vulnerabilities affect Sunway ForceControl 6.1 (SP1, SP2, and SP3) and pNetPower Version 6.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to perform a remote denial of service or to remotely execute arbitrary code against the ForceControl and pNetPower server applications. This action can result in adverse application conditions and ultimately impact the production environment on which the SCADA system is used.

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 environment, architecture, and product implementation.

BACKGROUND

Beijing-based Sunway ForceControl Technology Co. provides SCADA HMI applications for a variety of industries. Sunway's products are deployed primarily in China. According to the Sunway website,[d] the

a. NSS Labs, http://www.nsslabs.com, website last accessed June 16, 2011.

b. CWE-122: Heap-based Buffer Overflow, http://cwe.mitre.org/data/definitions/122.html, website last accessed June 16, 2011.

c. Sunway Security Bulletin, http://www.sunwayland.com.cn/news_info_.asp?Nid=3593, website last accessed June 16, 2011.

d. http://www.sunwayland.com.cn, website last accessed June 16, 2011.

products are also deployed in Europe, the Americas, Asia, and Africa. Sunway products are deployed across a wide variety of industries including petroleum, petrochemical, defense, railways, coal, energy, pharmaceutical, telecommunications, water, manufacturing, and others.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The following two vulnerabilities have been identified:

1. The heap-based buffer overflow affecting ForceControl 6.1 WebServer can be exploited if an attacker makes a request to the httpsvr.exe process with a specially crafted HTTP URL. Successful exploitation results in a denial of service and the possible execution of arbitrary code.
2. The heap-based buffer overflow affecting pNetPower AngelServer can be exploited if an attacker sends specially crafted UDP packets to the AngelServer.exe process. Successful exploitation results in a denial of service and the possible execution of arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

Remote exploitability of this vulnerability could be possible.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

Consistent exploit code is unlikely. An attacker would require at least an intermediate skill level to exploit this vulnerability.

MITIGATION

Sunway has developed patches for both vulnerabilities, available at the Sunway website:

1. For patching the ForceControl 6.1 WebServer URL request heap buffer overflow

   File Version: 6.0.5.3

   KB File Size: 27KB

   Published: May 20, 2011

   Download Address: http://www.eforcecon.com/download_view.asp?Nid=3594

   Validated by : CNVD

2. For patching the pNetPower 6.1 AngelServer UDP packet heap buffer overflow

   File Version: 6.0.11.3

   File Size: 32KB

   Published: May 20, 2011

   Download Address: http://www.eforcecon.com/download_view.asp?Nid=3595

   Validated by : CNVD

ICS-CERT encourages asset owners to 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.

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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a section for control system 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.*[e]

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.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed June 13, 2011.