ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-307-01—SCHNEIDER ELECTRIC VIJEO HISTORIAN WEB SERVER MULTIPLE VULNERABILITIES

November 28, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-307-01P on the US-CERT secure Portal on November 03, 2011. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of Security Research and Service Institute—Information and Communication Security Technology Center (ICST) has identified four vulnerabilities in the Schneider Electric Vijeo Historian product line. These vulnerabilities include a denial of service (DoS), buffer overflow, a cross-site scripting (XSS), and a directory traversal.

ICS-CERT has coordinated this report with Schneider Electric and ICST. Schneider has produced a fix that resolves these vulnerabilities. ICST has tested this fix and validated that it fully resolves these vulnerabilities.

AFFECTED PRODUCTS

According to Schneider Electric the following products are affected:

- Vijeo Historian V4.30 and earlier
- CitectHistorian V4.30 and earlier
- CitectSCADA Reports V4.10 and earlier.

IMPACT

Successful exploitation of these vulnerabilities could result in DoS, data leakage, or remote code execution.

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

Schneider Electric is a manufacturer and integrator of energy management equipment and software. According to Schneider Electric, its products are used worldwide. The Vijeo Historian, CitectHistorian, and CitectSCADA report products are data historian products. According to Schneider Electric, these products are used in energy, industry, and building automation.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DENIAL OF SERVICE

A buffer overflow vulnerability exists in the third-party TeeChart ActiveX control that could allow a remote attacker using social engineering to cause a DoS.

CVE-2011-4033[a] has been assigned to this vulnerability in the National Vulnerability Database (NVD).

BUFFER OVERFLOW

A buffer overflow vulnerability exists in the third-party TeeChart ActiveX control that could allow a remote attacker using social engineering to cause a denial of service and/or execute arbitrary code.

CVE-2011-4034[b] has been assigned to this vulnerability in the NVD.

CROSS-SITE SCRIPTING

A XSS vulnerability exists that could allow remote attackers using social engineering to inject arbitrary web script or HTML via an HTTP request.

CVE-2011-4035[c] has been assigned to this vulnerability in the NVD.

DIRECTORY TRAVERSAL

A directory traversal vulnerability exists in the web portal allowing remote attackers to read arbitrary files in an HTTP request.

CVE-2011-4036[d] has been assigned to this vulnerability in the NVD.

[a] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4033, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4034, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4035, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

VULNERABILITY DETAILS

EXPLOITABILITY

Three of these four vulnerabilities are remotely exploitable if used with social engineering. The directory traversal vulnerability can be exploited without social engineering.

EXISTENCE OF EXPLOIT

No publicly available exploits specifically targeting these vulnerabilities are known to exist.

DIFFICULTY

An attacker with a low to moderate skill level could potentially exploit these vulnerabilities.

MITIGATION

Schneider Electric has created a patch and has issued a customer notification describing the vulnerabilities.[e] Schneider Electric recommends that all customers using the above mentioned software packages download and apply the patch located at the below website: http://www.citect.com/index.php?option=com_content&view=article&id=1656&Itemid=1695

In addition to applying the patch developed by Schneider Electric, ICS-CERT encourages asset owners to take additional defensive measures against this and other cybersecurity threats by:

- Minimizing network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locating control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, using secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

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

[d] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4036 NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

[e] http://www.scada.schneider-electric.com/sites/scada/en/login/historian-vulnerability.page, website last accessed November 28, 2011.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[f]

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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[g] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[h] for more information on social engineering attacks.

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.

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 (ICSs) and the public at avoidable risk.

[f] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 28, 2011.

[g] Recognizing and Avoiding E-mail Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed November 28, 2011.

[h] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed November 28, 2011.