Advisory (ICSA-14-238-02)

Schneider Electric Wonderware Vulnerabilities

Original release date: August 26, 2014 | Last revised: August 27, 2014

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Timur Yunusov, Ilya Karpov, Sergey Gordeychik, Alexey Osipov, and Dmitry Serebryannikov of the Positive Technologies Research Team have identified four vulnerabilities in the Schneider Electric Wonderware Information Server (WIS). Schneider Electric has produced an update that mitigates these vulnerabilities.

Some of these vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following Schneider Electric WIS versions are affected:

- Wonderware Information Server 4.0 SP1 Portal,
- Wonderware Information Server 4.5 Portal,
- Wonderware Information Server 5.0 Portal, and
- Wonderware Information Server 5.5 Portal.

IMPACT

If these vulnerabilities are exploited, they could allow remote code execution, information disclosure, or session credential high jacking.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Schneider Electric corporate headquarters is located in Paris, France, and maintains offices in more than 100 countries worldwide.

The affected products, WIS software, provides industrial information content including process graphics, trends, and reports on a single web page. WIS web clients allow access to real-time dashboards, predesigned reports of industrial activities, and provide analysis or write back capabilities to the process. According to Schneider Electric, WIS is deployed across several sectors including Chemical, Commercial Facilities, Critical Manufacturing, Energy, Food and Agriculture, and Water and Wastewater Systems. Schneider Electric estimates that these products are used primarily in the United States and Europe with a small percentage in Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

ACCOUNT ENCRYPTION AND STORAGE[a]

Encryption of WIS is insufficient. If the attacker decrypts the credentials, an elevation of privilege could result. The system would need to be compromised for this attack to occur.

CVE-2014-2381[b] has been assigned to this vulnerability. A CVSS v2 base score of 2.1 has been assigned for local access; the CVSS vector string is (AV:L/AC:L/Au:N/C:P/I:N/A:N).[c]

CVE-2014-2380[d] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned for network access; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:N/A:N).[e]

CROSS-SITE SCRIPTING[f]

WIS fails to validate, filter, or encode user input before returning it to a user's web client.

CVE-2014-5397[g] has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).[h]

IMPROPER INPUT VALIDATION[i]

WIS may allow access to local resources (files and internal resources) via unsafe parsing of XML external entities. By using specially crafted XML files, an attacker can cause these products to send the contents of local remote resources to the attacker's server or cause a denial of service of the system. This vulnerability is not exploitable remotely and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed XML files.

CVE-2014-5398[j] has been assigned to this vulnerability. A CVSS v2 base score of 2.1 has been assigned; the CVSS vector string is (AV:L/AC:L/Au:N/C:P/I:N/A:N).[k]

SQL INJECTION[l]

WIS is vulnerable to a SQL injection vulnerability by performing database operations that were unintended by the web application designer and, in some instances,

can lead to compromise of the database server or lead to remote code execution.

CVE-2014-5399[m] has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).[n]

VULNERABILITY DETAILS

EXPLOITABILITY

Some of these vulnerabilities could be exploited remotely.

The Improper Input Validation is not exploitable remotely and does require user interaction. This particular vulnerability is only triggered when a local user runs the vulnerable application and loads the malformed XML file.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

Crafting a working exploit for some of these vulnerabilities would be difficult. Social engineering is required to convince the user to accept the malformed XML file. Additional user interaction is needed to load the malformed file. This decreases the likelihood of a successful exploit.

MITIGATION

Schneider Electric has created an update for WIS web pages and components to address the vulnerabilities listed in this advisory. Customers using all versions of WIS are affected and should upgrade to WIS Version 5.5 and then apply the security update.

Customers using the affected versions of WIS should set the security level settings in the Internet browser to “Medium – High” to minimize the risks presented by these vulnerabilities. In addition, the Wonderware Information Server Portal can be configured to use HTTPS that will require additional steps as documented in the products user documentation.

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 and/or systems, and ensure that they are not accessible from 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize 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 at: http://ics-cert.us-cert.gov/content /recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

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 email messages.
2. Refer to Recognizing and Avoiding Email Scams[o] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[p] for more information on social engineering attacks.

---

a. CWE-326: Inadequate Encryption Strength, http://cwe.mitre.org/data/definitions/326.html, web site last accessed August 26, 2014.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2381, 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:L/AC:L/Au:N/C:P/I:N/A:N, web site last accessed August 26, 2014.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2380, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

e. 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 accessed August 26, 2014.

f. CWE-79: Improper Neutralization of Input During Web Page Generation (“Cross-site Scripting”), http://cwe.mitre.org/data/definitions/79.html, web site last accessed August 26, 2014.

g. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5397, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

h. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:P/I:P/A:P, web site last accessed August 26, 2014.

i. CWE-20: Input Validation, http://cwe.mitre.org/data/definitions/20.html, web site last accessed August 26, 2014.

j. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5398, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

k. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:L/AC:L/Au:N/C:P/I:N/A:N, web site last accessed August 26, 2014.

l. CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), http://cwe.mitre.org/data/definitions/89.html, web site last accessed August 26, 2014.

m. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5399, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

n. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:P/I:P/A:P, web site last accessed August 26, 2014.

o. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, web site last accessed August 26, 2014.

National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, web site last accessed August 26, 2014.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.