ICS-CERT ADVISORY

ICSA-12-213-01—SIELCO SISTEMI WINLOG MULTIPLE VULNERABILITIES

July 31, 2012

OVERVIEW

This advisory is a follow-up to the alerts titled "ICS-ALERT-12-166-01—Sielco Sistemi Winlog Buffer Overflow" that was published June 14, 2012, and "ICS-ALERT-12-179-01—Sielco Sistemi Winlog Multiple Vulnerabilities" that was published June 27, 2012, on the ICS-CERT Web page.

Researchers Carlos Mario Penagos Hollmann of IOActive, Michael Messner, and Luigi Auriemma have separately identified multiple vulnerabilities in Sielco Sistemi's Winlog application. Sielco Sistemi has produced a new release that corrects all identified vulnerabilities. Mr. Hollmann and Mr. Auriemma have tested the release to validate that it resolves the vulnerabilities. These vulnerabilities can be remotely exploited. Exploit code is publicly available for these vulnerabilities.

AFFECTED PRODUCTS

The following Sielco Sistemi products are affected.

- Winlog Pro SCADA, all versions prior to 2.07.18
- Winlog Lite SCADA, all versions prior to 2.07.18.

IMPACT

Successful exploitation of these vulnerabilities could lead to a program crash, information leakage, or arbitrary 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

Sielco Sistemi is an Italy-based company that creates supervisory control and data acquisition (SCADA)/human-machine interface (HMI) software and hardware products.

Winlog Lite SCADA is a demo version of the Winlog Pro SCADA/HMI system. According to Sielco Sistemi, Winlog Pro SCADA is deployed across several sectors including manufacturing, public utilities, telecommunications, and others. Sielco Sistemi products are deployed mainly in Italy, Turkey, Canada, USA, Indonesia, and Spain.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

FAILURE TO CONSTRAIN OPERATIONS WITH THE BOUNDS OF A MEMORY BUFFER[a]

By sending malicious specially crafted packets to Port 46824/TCP, an attacker can overflow a memory buffer on the target system. Errors in RunTime.exe and TCPIPS_Story.dll can be exploited by these packets to cause the buffer overflow. The packets can also cause a boundary error in RunTime.exe causing the buffer overflow. This can allow the attacker to cause a denial-of-service condition leading to a crash or possible execution of arbitrary code.

CVE-2012-3815[b] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[c]

IMPROPER ACCESS CONTROL[d]

Unauthorized users can access and read files on the system that Winlog is running by causing an input validation error. An attacker can send a malicious specially formed packet to Port 46824/TCP to allow unauthorized access to the system, which may lead to information leakage.

[a] CWE-119: Failure to Constrain Operations within the Bounds of a Memory Buffer, http://cwe mitre.org/data/definitions/119.html, Web site last accessed July 31, 2012.

[b] NVD, http://web.nvd nist.gov/view/vuln/detail?vulnId=CVE-2012-3815 , Web site last accessed July 31, 2012.

[c] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last accessed July 31, 2012.

[d] CWE-284: Improper Access Control, http://cwe mitre.org/data/definitions/284 html, Web site last accessed July 31, 2012.

CVE-2012-3815[b] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C). [c]

IMPROPER ACCESS OF INDEXABLE RESOURCE[e]

By sending malicious specially crafted packets that point outside of the defined array, an attacker can cause a crash of the system. By using 32-bit operation coding, a file pointer outside the array can be used to execute arbitrary code and cause a denial-of-service condition leading to a crash.

CVE-2012-3815[b] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[c]

WRITE-WHAT-WHERE CONDITION[f]

By sending a malicious specifically formed packet, unauthorized attackers are able to write outside of the existing buffer allocation. The error when allocating when processing these malicious packets can be exploited to reference an invalid memory location. This exploit could cause a crash of the system.

CVE-2012-3815[b] has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).[c]

Some of the preceding vulnerability details were obtained from a Secunia Advisory SA49395.[g]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities can be remotely exploited.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

An attacker with a low-skill level would be able to exploit these vulnerabilities.

[e] CWE-118: Improper Access of Indexable Resource, http://cwe.mitre.org/data/definitions/118 html, Web site last accessed July 31, 2012.

[f] CWE-123: Write-what-where Condition, http://cwe mitre.org/data/definitions/123 html, Web site last accessed July 31, 2012.

[g] Secunia Advisory SA49395, http://secunia.com/advisories/49395, Web site last accessed July 31, 2012.

MITIGATION

Sielco Sistemi has created an update to fix these vulnerabilities. This update, Winlog Pro SCADA and Winlog Lite SCADA Version 2.07.18, is available for customer download at the following location: http://www.sielcosistemi.com/en/news/index.html?id=70

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.

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.[h] 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[i] 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 CSSP Information and Incident Reporting: www.ics-cert.org

[h] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 31, 2012.

[i] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed July 31, 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.