



ICS-CERT ALERT

ICS-ALERT-11-332-02—SIEMENS SIMATIC WINCC FLEXIBLE VULNERABILITIES

November 28, 2011

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting Siemens SIMATIC WinCC Flexible Runtime, a human-machine interface product. According to this report, the vulnerabilities are exploitable remotely via Port 2308/TCP. This report was released by Luigi Auriemma without coordination with ICS-CERT, the vendor, or other coordination entity that ICS-CERT is aware of.

ICS-CERT has coordinated the report with Siemens, who is working to confirm the report and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report includes details and PoC exploit code for the following vulnerabilities:

| Vulnerability Type | Exploitability | Impact |
|---------------------|----------------|--------------------------------|
| Stack Overflow | Remote | Possible Remote Code Execution |
| Directory Traversal | Remote | Read, Write, Delete Access |
| Memory Read Access | Remote | Denial of Service |

ICS-CERT and Siemens are currently evaluating the reported stack overflow vulnerability, which may be the same as a previously reported vulnerability.^a

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

BACKGROUND

Siemens SIMATIC WinCC flexible is a software package used for visualization and machine or small system operations. This product runs on standard PCs or on Siemens panel PCs. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical.

MITIGATION

ICS-CERT is currently coordinating with the vendor to identify mitigations.

a. http://www.uscert.gov/control_systems/pdf/ICSA-11-244-01.pdf, website last accessed November 28, 2011.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Configure firewall rules appropriately for traffic on Port 2308/TCP.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.^b
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ 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.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.^c

Organizations that observe 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

ICS-CERT Operations Center

1-877-776-7585

ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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 declines attribution. 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.

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed November 28, 2011.

c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 28, 2011.