



ICS-CERT ALERT

ICS-ALERT-11-336-01—3S CODESYS WEBSERVER BUFFER OVERFLOW

December 02, 2011

ALERT

SUMMARY

ICS-CERT is aware of public reporting of a buffer overflow vulnerability with proof-of-concept (PoC) exploit code affecting 3S CoDeSys web server, a Supervisory Control and Data Acquisition/Human-Machine Interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable by sending specially crafted packets to the server Port 8080/TCP. This report was released by Celil Unuver of SignalSEC Labs.

ICS-CERT had been coordinating the vulnerability with the security researcher and affected vendor prior to the public release. ICS-CERT is issuing this alert to provide notice of the report and identify baseline mitigations for reducing risks to this and other cybersecurity attacks.

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

Vulnerability Type	Exploitability	Impact
Buffer Overflow	Remote	Denial of Service/Possible Remote Code Execution

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

MITIGATION

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

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

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.^a
- 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.

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



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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

The Control Systems Security Program 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*.^b

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 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.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 01, 2011.