ICS-CERT ALERT

ICS-ALERT-13-016-02—OFFLINE BRUTE-FORCE PASSWORD TOOL TARGETING SIEMENS S7

January 16, 2013

ALERT

SUMMARY

ICS-CERT is aware of a public report of an offline brute-force password tool with proof-of-concept (PoC) exploit code targeting Siemens S7 programmable logic controllers. According to this report, a password can be obtained by offline password brute forcing the challenge-response data extracted from TCP/IP traffic file. This report was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the attack vector 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 included details and PoC exploit code for the following exploit tool:

Exploit Tool	Impact
Credentials Brute Force	Possible capture of current credentials for device

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

Alexander Timorin and Dmitry Sklyarov of SCADA Strangelove[a] claims to have announced at the S4 security conference, a Python programming code[b] that may brute force captured TCP/IP traffic to narrow down and expose the credentials from challenge-response protocol.

An attacker must be on an adjacent network to be able to capture this traffic. The possibility exists that this code may be modified to be used against other vendor products.

a. Web site, http://scadastrangelove.blogspot.ru/, Web site last visited January 16, 2013.
b. PasteBin Web site, http://pastebin.com/0G9Q2k6y, Web site last visited January 16, 2013.

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 this attack vector. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[c]
- 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.

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[d]

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
Email: ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting: www.ics-cert.org

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/.

c. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed January 16, 2013.

d. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 16, 2013.

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 attribution provided to researchers? Attribution for discovery is always provided to the reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate details before public release. The public release of details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.