ICS-CERT ALERT

ICS–ALERT-11-111-01—GLEG AGORA SCADA+ EXPLOIT PACK UPDATE 1.1

April 21, 2011

ALERT

SUMMARY

On April 21, 2011, GLEG Ltd. announced update Version 1.1 for the Agora SCADA+ Exploit Pack for Immunity's CANVAS system. CANVAS is a penetration testing framework that is extensible using CANVAS Exploit Packs.

This update includes two new zero-day exploits:

- Beckhoff TwinCAT ENI Server Version 1.1.6.0 – SCADA exploit
- Iconics GENESIS32 and GENESIS64 GenBroker.exe – Denial of Service.

Exploits for five additional control system products are also included in this update. These additional exploits are known vulnerabilities for which ICS-CERT has recently published advisories.

ICS-CERT has notified the affected vendors. ICS-CERT has also reached out to GLEG for additional information, but GLEG has declined to provide further details of the vulnerabilities.

MITIGATION

ICS-CERT recommends that users minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[1] 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).

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

1. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 2011.

The Control System 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.*[2]

BACKGROUND

Immunity's CANVAS is a penetration framework similar to the popular Metasploit tool. GLEG is a small company based in Moscow, Russia, that produces add-on exploit packages for CANVAS.

ICS-CERT CONTACT

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

ICS-CERT Operations Center
1-877-776-7585

www.ics-cert.org
ICS-CERT@DHS.GOV

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.

2. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html