ICS-CERT ALERT

ICS-ALERT-12-019-01A—GE D20ME PLC MULTIPLE VULNERABILITIES

UPDATE A

April 09, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting the General Electric (GE) D20ME, part of the GE D20Substation Controller product. According to this report, the vulnerability is exploitable by using TFTP connections to the controller. This report is based on information presented by Reid Wightman during Digital Bond's SCADA Security Scientific Symposium (S4) on January19, 2012, without coordination with either the vendor or ICS-CERT.

--------- Begin Update A Part 1 of 3 --------

Reid Wightman, of Digital Bond, has released Metasploit modules to exploit the vulnerabilities outlined in this alert.

Newly Released Metasploit module[a]:

- **d20_tftp_overflow :** triggers a Denial of Service condition due to a buffer overflow vulnerability in GE's D20ME PLC TFTP server.

--------- End Update A Part 1 of 3----------

ICS-CERT has notified GE of the report and has asked GE to confirm the vulnerability 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 vulnerability details and PoC exploit code for the following vulnerabilities:

Vulnerability Type	Exploitability	Impact
Data leakage	Remote	Data leakage of authentication credentials.
Arbitrary Code Execution	Remote	Attacker can execute arbitrary commands/Denial of Service
--------- Begin Update A Part 2 of 3 --------		

a. https://community.rapid7.com/community/metasploit/blog/2012/04/05/metasploit-update, website last accessed April 09, 2012.

Buffer Overflow	Remote	Denial of service with potential of arbitrary code execution
--------- End Update A Part 2 of 3----------		

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

MITIGATION

ICS-CERT is currently coordinating with GE and the security researcher to identify mitigations.

--------- Begin Update A Part 3 of 3 --------

GE requests that users contact their GE support representative for additional mitigation information for these vulnerabilities.

--------- End Update A Part 3 of 3----------

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.[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.

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed April 09, 2012.
c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 09, 2012.

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.