Digital Energy
MDS

PRODUCT BULLETIN

NUMBER: PB15007_B

August 2015

PulseNET
ICS-CERT Advisory: ICS-VU-629115
and
ICS-CERT Advisory: ICS-VU-622389

GE MDS, LLC., 175 Science Parkway, Rochester, NY 14620 USA
Phone +1 (585) 242-9600, FAX +1 (585) 242-9620

HARD-CODED CREDENTIALS VULNERABILITY AND DIRECTORY TRAVERSAL VULNERABILITY

Introduction

Two vulnerabilities have been identified in components used by the PulseNET Network Management Software. This product bulletin discusses the vulnerabilities and announces the release of software versions that resolve them. These issues affect PulseNET and PulsetNET Enterprise versions 3.1.3 and all previous versions.

The first is a hard-coded credentials vulnerability that would allow administrative access to the software. A support account included as default in the software could allow complete control of the PulseNET system, including the ability to run arbitrary code, to an attacker who knows these credentials.

The second is a directory traversal vulnerability within the web application that would allow a user to read and delete arbitrary files on the PulseNET system.

GE Digital Energy has validated the existence of these vulnerabilities and is providing a product update that resolves both issues. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has issued advisories tracking these issues, identified as ICS-VU-629115 and ICS-VU-622389.

Product Background

PulseNET is a software application used for monitoring devices in Industrial Communications networks. Each device that PulseNET monitors serves a specific function in the network. These functions may include acting as a bridge, router, access point/base station, or remote/subscriber. The devices can be widely dispersed geographically and are able to operate with different bandwidths, depending on radio type and frequency.

Vulnerability Overview

Installation of PulseNET includes a default support user account that grants administrative access to the PulseNET software. Pulsenet also includes administrative features that may be used to remotely execute arbitrary code. If known to an attacker, the support account credentials could allow an attacker to execute code as the system user that started the PulseNET service. This vulnerability is identified by ICS-CERT as ICS-VU-629115.

PulseNET provides file download functionality through a web application page. A vulnerability in this page allows a user to supply a file path to any file on the server, which is transferred to the user. An attacker could use this vulnerability to transfer any arbitrary file from the PulseNET system to the user in addition to deleting the file from the server. This vulnerability is identified by ICS-CERT as ICS-VU-622389.

Mitigation

GE encourages our customers to update PulseNET to the latest published version. Software version 3.1.5 eliminates these vulnerabilities. Updates for PulseNET are available at: http://www.gedigitalenergy.com/Communications/MDS/PulseNET_Download.aspx.

Updates to PulsetNET Enterprise are available at:
http://www.gedigitalenergy.com/Communications/MDS/PulseNETEnt_Download.aspx

Acknowledgements

GE would like to thank Andrea Micalizzi (rgod) working with HP's Zero Day Initiative for reporting these issues via ZDI and ICS-CERT and for helping to protect our customers.

GE Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact the PSIRT at www.ge.com/security or security@ge.com.

Product Support

GE Digital Energy is committed to the continued support of the MDS product line. We appreciate your business and look forward to continuing to grow our relationship.
If you need help with any aspect of your GE Digital Energy product, you have a few options:

Search Technical Support

The GE Digital Energy Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics. Visit us on the Web at:
http://www.gedigitalenergy.com/

Contact Customer Service

The GE Digital Energy Customer Service Center is open 24 hours a day, seven days a week for you to talk directly to a GE representative.
In the U.S. and Canada, call toll-free: 1-800-547-8629
International customers please call: + 1-905-294-6222
Or e-mail to: **ge4service@ge.com**