



GE VERNOVA

SSH and EAP-TTLS Login Vulnerability

UR Product Line

Security Notice

Date: 26 September 2016

Last updated: 22 January 2018

ID: UR-2016-000003-3

Classification: Confidential

CVSS: (AV:N/AC:M/Au:N/C:P/I:N/A:P)

Overview

A report by Kaspersky Labs identifies a “buffer overflow” vulnerability in the GE Vernova UR product line, that an attacker could exploit the UR login feature with either direct or remote access to the UR device. This vulnerability affects UR platform devices using firmware versions 7.01 to 7.32 with the SSH and EAP-TTLS login features enabled. SSH and EAP-TTLS features are only available in UR devices with the CyberSentry software option.

A UR device uses the Secure Shell (SSH) protocol to allow remote access to the device. EAP-TTLS is used as the RADIUS authentication method, when the “Server” Authentication type is selected for login.

GE Vernova recommends upgrading to firmware version 7.41 or higher to resolve this issue.

Vulnerability Details

A buffer overflow can occur in the login function of SSH & EAP-TTLS features in UR CyberSentry. Successful exploitation of this vulnerability could lead to a remote arbitrary code execution. And this type of vulnerability could be remotely exploited.

The UR family of products with firmware version from 7.01 to 7.32 is susceptible to this vulnerability.

Mitigation

GE Vernova recommends that all users update their UR devices to version 7.41 or higher to resolve this issue.

It is recommended that users evaluate their current risk and implement appropriate network security mitigation measures including:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

GE Vernova Product Security Incident Response Team (PSIRT)

GE Vernova 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.gevernova.com/security or GEV.PSIRT@gevernova.com.

Product Support

GE Vernova Grid Solutions is committed to the continued support of the UR 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 Vernova Grid Solutions product, use the following options:

Search Technical Support

The GE Vernova Grid Solutions Web site provides fast access to technical information, such as manuals, release notes, and knowledge base topics. Visit us on the Web at: <https://www.gevernova.com/grid-solutions>

Contact Customer Service

The GE Vernova Grid Solutions Customer Service Center is open 24 hours a day, seven days a week for you to talk directly to a GE Vernova 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@gevernova.com