UCSC Controller Unauthorized Data Access

Date: October 22, 2018

Overview:

A security vulnerability has been identified in the Mark* VIe UCSCH1x and UCECH1x CPUs that if successfully exploited could allow unauthorized access to restricted areas of the controller.

The UCSC controller supports multiple independent operating systems running simultaneously on the Mark VIe control hardware.

The overall CVSS score calculated for this vulnerability is 8, based on the CVSS V3 vector:

AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N/E:H/RL:O/RC:C/CR:H/IR:X/AR:X/MAV:N/MAC:H/MPR:LM UI:N/MS:C/MC:H/MI:N/MA:N

This issue is isolated in some firmware versions and hardware platforms with ControlST* Software Suite V07.00 through V07.03.

Table 1. Affected Products

ControlST Version:	Hardware Platform
V07.00	UCSCH1x
V07.01	UCSCH1x
V07.02	UCSCH1x
V07.03	UCSCH1x, UCECH1x

Environment:

- Mark* VIe, EX2100e
- EX2100e Regulator
- LS2100e
- UCSCH1x Controller
- UCECH1x

Recommendations:

Sites running ControlST V07.01 through V07.03 should upgrade to the latest ControlST Service Pack or the highest version available. Sites running ControlST V07.00 should upgrade, at minimum, to the latest ControlST V07.01 release. The issue has been resolved in ControlST

V07.01 through V07.03 listed in the table below. These contain the required product versions to eliminate the issue.

Table 2. ControlST Package Versions to Upgrade To

If ControlST Version currently installed is:	Upgrade to:
V07.00	V07.01.01C SP10
V07.01	V07.02.00C SP06
V07.02	V07.02.07C
V07.03	V07.03.01C

Please, contact your local GE Service Representative to obtain the applicable ControlST version.

To minimize the risk of exposure to this and any other vulnerabilities, GE recommends a defense-in-depth approach to protecting critical process control equipment. Guidance on technology and best practices to secure GE controllers from Cyber-attack are provided in the Mark VIe Control Systems Secure Deployment Guide (GEH-6839), which can be requested through GE Service Representative. For best maintenance practices on cyber risks, please refer to GEK 121594.

*Trademark of General Electric Company

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0026290

GE Power 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 GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.