Mark* VIe Web Server Update (ICSA-18-347-04)

Date: December 18, 2019

Summary:

A security vulnerability has been identified in the Mark* VIe Control and associated products, including the EX2100e Excitation Control, Automatic Voltage Regulator (AVR), and LS2100e Static Starter Control. The Mark VIe control implements a web service that provides access to various web clients, including HMIs panel-mounted touch screens for excitation monitoring and control. The web server that provides this feature allows access to system files beyond the web server root directory. Using directory traversal methods, an attacker may be able to access system data, which could result in escalation of privilege and unauthorized access to the controller.

The base CVSS score calculated for this vulnerability is 7.4, based on the CVSS V3 vector **(CSVS V3 7.4)**: /AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

The path traversal vulnerability has been corrected in firmware versions listed in table 1 shown below.

Environment:

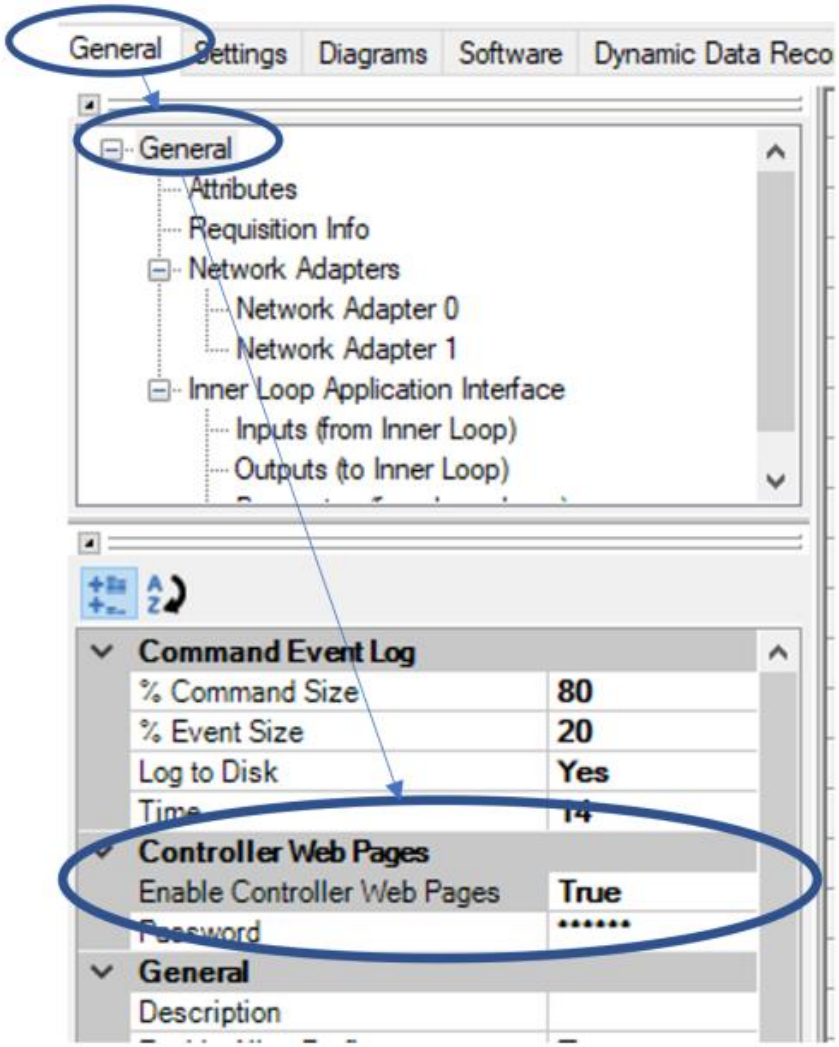
- Mark VIe, EX2100e
- LS2100e ControlST* Software Suite

Resolution:

In applications where the controller-hosted web server is not required, GE recommends turning off the web server. Refer to GEH 6700 for more details on how to disable this. In summary:

- Go to the device software
- Click the general tab
- In the "General" section, go to the "Controller Web Pages" and set it to FALSE.

Example:



For all other applications, GE recommends updating the controller to the ControlST version in Table 1 below or later.

Table 1. Controls ST Package Version to Upgrade To

Product	ControlST Version
Mark VIe	V05.04.00C
EX2100e	V06.00.00C
EX2100e_Reg	V06.00.00C
LS2100e	V06.00.00C

Please, contact your local GE Service Representative for assistance in implementing a ControlST update.

GE recommends that all standalone Excitation Controls be segmented from other networks using a firewall installed inside the Excitation panels. External communication should be exclusively restricted to only those protocols specifically required for command and control, such as Modbus®. Other services including HTTP must be blocked from external access.

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 your local GE Service Representative. For best maintenance practices on cyber risks, please refer to GEK 121594.

*Trademark of General Electric Company

Attachments

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0026288

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.