GE (M&D) Statement on Customer Cyber Security Concerns: SolarWinds Breach

Date: December 31, 2020

Introduction

Providing a secure and reliable remote monitoring of the customers' controllers is vital to the operations of GE M&D. Our goals are to operate our services with security as a key principle. We have implemented and will maintain reasonable and appropriate technical and organizational measures, internal controls, and information security routines intended to help protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction.

Customer Security Concern

SolarWinds recently (Dec 13, 2020) announced a Security Advisory that specifies that they were the victims of a cyberattack that resulted in attackers embedding malware into updates to SolarWinds Orion software. GE M&D uses SolarWinds for infrastructure administration including the OSM server at customer sites.

GE M&D Response

GE M&D has shown no signs of being impacted by this breach. There have been no signs of attackers gaining access to M&D's SolarWinds Orion server and no beaconing activity on our network related to known attacker C2 channels. GE updated our Orion server with the patch that SolarWinds has provided (2020.2.1 HF 1). We were running the vulnerable 2020.2 version

of SolarWinds Orion from June of this year until November. We have provided a table that covers the timeline of our upgrades to our Orion server.

Upgrade Date	Version
June 3, 2019	Orion Platform 2018.4
May 12, 2020	Orion Platform 2019.4
June 18, 2020	**Orion Platform 2020.2**
November 23, 2020	Orion Platform 2020.2.1
November 25, 2020	Orion Platform 2020.2.1. HF1

Table 1. Timeline of M&D's SolarWinds Orion Updates

GE has taken our SolarWinds server offline for the foreseeable future in order to perform forensic due diligence to make 100% sure we are not compromised. GE will update our Orion server with the HotFix that SolarWinds says it will provide on December 15, 2020 to fully remediate the issues.

Our customer's security is a top priority at M&D and it is part of our Incident Response plan to notify any customer immediately if they are involved in any cyber incident. GE does not believe that we or any of our customers are involved in this cyber incident. We will notify customers if this view changes.

References

https://www.solarwinds.com/securityadvisory

https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

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.