NERC Lessons Learned

Kevin Hatch
Manager, Reliability Engineering

NERC Lessons Learned

- Loss of Energy Management System Functionality due to Server Resource Deadlock
  - Lesson Learned #: LL20220901
  - Date Published: September 28, 2022
  - Category: Communications
  - Loss of EMS Functionality due to Server Resource Deadlock

Loss of Energy Management System Functionality

Problem Statement

- An antivirus software engine installed on energy management system (EMS) production servers had a flaw that caused affected servers to deadlock server resources and become unresponsive, effectively making the EMS unavailable to operators.
- The flaw was not recognized in test environments due to the difference in input/output (I/O) workload on test servers versus those seen on production servers

Details

- Two separate events over the span of two weekends led to a period of 31 consecutive minutes of complete loss of EMS functionality; this occurred again on the following Saturday for a period of 81 consecutive minutes.
- These performance degradation events removed the ability to control Bulk Electric System (BES) elements at the impacted substations, and the entity was unable to calculate Reporting Area Control Error (ACE), control performance standards, or implement automatic generation control. The entities' state estimator (SE) and real-time contingency analysis (RTCA) were not solving, and real-time monitoring and alarming was not functioning on the EMS

Forecasted High Winds

Corrective Actions

- The entity disables select services and uninstalled the flawed malware engine.

Lessons Learned

- Vendor assertions should be tested in a more rigorous way before concluding they are the correct root cause
- Shared Physical Space Enabled Complex Troubleshooting
- Remote Connectivity Sped Initial Response
- Have Central Incident Response Tooling and Training

Contact

Presenter:
Kevin Hatch, Kevin.Hatch@pjm.com

SME:
Kevin Hatch, Kevin.Hatch@pjm.com

NERC Lessons Learned

Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com

PROTECT THE POWER GRID

THINK BEFORE YOU CLICK!

Be alert to malicious phishing emails.

Report suspicious email activity to PJM.

(610) 666-2244 / it_ops_ctr_shift@pjm.com