CO-OPS Engineering Bulletin 15-003

Engineering Change: Review station system logs for suspicious activity when performing troubleshooting of a CO-OPS data collection system.

Systems Affected: All CO-OPS observing systems

Originating Team: Chesapeake Instrument Lab

MSCS Approval Date: December 15, 2015

Background: CO-OPS data collection systems implement multiple means of communications for system maintenance and data retrieval. These communications means can be susceptible to access attempts by third parties with possible malicious intent. These attempts are normally from automated systems which will use common user name and password combinations to attempt to gain access. While attempting to access a system using this method there will be a high number of unsuccessful login attempts over an extended period of time which has the potential of causing system performance issues and can interfere with CO-OPS' ability to communicate with the systems.

Action Required: When investigating issues at a station the system logs should be reviewed for any unusual activity which may indicate a third party attempt to access the system. This type of activity will normally appear as failed login attempts using commonly used user names and passwords. Any suspicious activity should be reported immediately via email to the following recipients:

chris.mcgrath@noaa.gov
kevin.harrison@noaa.gov
robert.heitsenrether@noaa.gov
caleb.gostnell@noaa.gov

This email should include the station number, station name, a description of the issue at the station, the station IP address and/or phone number, and an exported copy of the system log. This group will then assess the unusual activity, coordinate with the telecommunications provider, and report out to the appropriate IT personnel and CO-OPS management.

Estimated Time To Complete: 15 minutes per troubleshooting session

References:

3.2.3.9 I10 EB 07-007 Exporting Xpert Data Using Xterm