December 20, 2021   JCI-PSA-2021-24
                                                                     CVE-2021-44228
                                                                     ICSA-21-357-02

Overview
Johnson Controls has confirmed the presence of a vulnerable version of Log4J, which may be exposed via exacq Enterprise Manager. Enterprise Manager customers are encouraged to upgrade to the latest exacq release to prevent any remote code execution. Alternatively, there is a work around that can be applied in the short term.

Impact
An attacker could enter malicious input and potentially allow remote code execution.

Affected Versions
- All versions of exacq Enterprise Manager up to and including version 21.12

Mitigation
- Upgrade exacq Enterprise Manager to version 21.12.1.
  -or-
- Apply manual mitigation steps (available on request)

Refer to the exacq Hardening Guide for guidance on isolating exacqVision NVRs and Enterprise Manager from public facing networks to reduce network exposure to attacks.
https://www.johnsoncontrols.com/cyber-solutions/cyber-learning

Initial Publication Date
December 20, 2021

Last Published Date
December 20, 2021

Resources
Cyber Solutions Website - https://www.johnsoncontrols.com/cyber-solutions/security-advisories
CVE-2021-44228 - NIST National Vulnerability Database (NVD) and MITRE CVE® List
ICSA-21-357-02 - CISA ICS-CERT Advisories

The power behind **your mission**