Log4j Vulnerability Advisory

This notification is to inform you of the availability of Attivo Software builds that address the recently disclosed **Log4j vulnerability** (https://nvd.nist.gov/vuln/detail/CVE-2021-44228).

While Attivo products (BOTsink, Attivo Central Manager and Attivo Cloud) do utilize Log4j, they are not vulnerable as we are using a newer version of JAVA which prevents remote execution. The severity of this vulnerability should be low if Attivo's products, specifically BOTsink or Attivo Central Manager have been deployed inside of the Enterprise behind a firewall that is patched to handle/block this vulnerability. In addition, one can use "Access Control" capability in Attivo Central Manager and BOTsink to limit who can access these devices.

Plan of action to address this vulnerability:

1. For customers who are currently on any version of 5.0.1.xx or 5.5.0.xx on BOTsink, ACM, or EDNM (and have a connection with the Update Server)
    - Check for the latest upgrade by clicking "Check Now" on the Administration->System Page
    - Download and upgrade the version offered
2. For customers on previous release versions
    - Contact Attivo Support for assistance to manually address the vulnerability
      OR
    - Upgrade to build 5.0.1.141 (should be available on our Support Portal by the end of the day today, 12/13)
3. For customers on the FIPS version
    - FIPS versions of the Attivo software that address this vulnerability are not currently available.
    - Attivo will provide an update and expected availability date as soon as possible.
4. For customers who don't want to upgrade software
    - the Attivo Support team will be able to assist with the necessary configuration updates on your devices to prevent this vulnerability. Please log a support ticket to request assistance.

Important Notes:

- This vulnerability is relevant to Attivo management platforms only. Therefore, neither Endpoint Detection Net (EDN) endpoints nor the ThreatDirect VM products are affected by this vulnerability.
- The Attivo Cloud SaaS solutions have already been updated to prevent this vulnerability from being exploited.

Please reach out to Attivo Support if you have any questions, concerns, or issues.