IASME VULNERABILITY DISCLOSURE POLICY

IASME are committed to addressing and reporting security issues through a coordinated and constructive approach designed to provide the greatest protection for IASME customers, partners, staff and all Internet users. This policy applies to vulnerabilities discovered anywhere by IASME staff and by others in IASME services.

If you believe you have discovered a vulnerability in a IASME service or have a security incident to report, please email us at security@iasme.co.uk or fill out this contact form: https://www.iasme.co.uk/contact-us.

We appreciate the use of the Common Vulnerability Scoring System: https://www.first.org/cvss/calculator/3.1.

Once we have received a vulnerability report, IASME takes a series of steps to address the issue:

1. IASME requests the reporter keep any communication regarding the vulnerability confidential.

2. IASME investigates and verifies the vulnerability.

3. IASME addresses the vulnerability and releases an update or patch within 90 days. If for some reason this cannot be done within this timeframe or at all, IASME will provide information on recommended mitigations.

4. IASME publicly announces the vulnerability in the release notes of the update. IASME may also issue additional public announcements, for example via social media.

5. Release notes (and blog posts when issued) include a reference to the person/people who reported the vulnerability, unless the reporter(s) would prefer to stay anonymous.

IASME will endeavour to keep the reporter apprised of every step in this process as it occurs. We greatly appreciate the efforts of security researchers and discoverers who share information on security issues with us, giving us a chance to improve our services, and better protect our customers. Thank you for working with us through the above process.

Once we have found a vulnerability in another vendor's products, IASME takes a series of steps to address the issue:

1. IASME will convene their vulnerability analysis team. This team, led by the CTO, is solely responsible for determining the severity of the vulnerability and managing the disclosure process.

2. IASME will keep any communication confidential regarding the vulnerability until the completion of the disclosure process.

3. IASME will attempt to contact the appropriate product vendor by email and telephone.

4. IASME will provide the vulnerability details to the vendor.

IASME will prepare and publish an advisory detailing the vulnerability at least 90 days after initial attempts at disclosure at stage 2 above, barring extenuating circumstances. This advisory will be made available to the general public via IASME's social media.