Chess Vulnerability Disclosure Policy

At Chess, we are committed to ensuring the security and integrity of our systems and data. We recognize the valuable role that security researchers and the broader community play in identifying vulnerabilities and helping us improve our security posture. This Vulnerability Disclosure Policy outlines our approach to receiving and handling vulnerability reports.

Scope

This policy applies to any vulnerabilities you are considering reporting to us (the "Organisation"). We encourage the responsible disclosure of security vulnerabilities in our systems, services, and products.

Reporting a Vulnerability

If you believe you have discovered a security vulnerability in any of our systems, services, or products, please report it to us by following these steps:

1. **Contact Information**: Send an email to customerservices@chessict.co.uk with the subject line "Vulnerability Disclosure".
2. **Include Details**: Provide a detailed description of the vulnerability, including the following information:
    - The type of vulnerability and its potential impact.
    - Detailed steps to reproduce the vulnerability. Ensuring such steps are a benign and non-destructive proof of concept.
    - Your contact information for follow-up.

What to Expect

Upon receiving your report, you can expect the following:

1. **Acknowledgement**: We aim to acknowledge receipt of your vulnerability report within 5 working days.
2. **Assessment**: Our security team will assess the report and determine the severity and impact of the vulnerability.
3. **Communication**: Where a finding is sufficiently severe/complex, we aim to keep you informed of our progress. However, priority for remediation is assessed on a case-by-case basis and may take some time to triage or fully address. You are welcome to enquire on the status but should avoid doing so more than once every 14 days.
4. **Resolution**: Once resolved, we aim to notify you of its resolution and may be in touch further to confirm the solution covers the vulnerability sufficiently.

Recognition

Please note that Chess does not offer a formal bug bounty program or reward for vulnerability reports. However, we greatly appreciate the efforts of security researchers and the broader community in helping us improve our security.

Responsible Disclosure

By submitting a vulnerability report, you agree to disclose the vulnerability in good faith, without malicious intent and **will NOT:**

1. Break any applicable law or regulations.
2. Publicly disclose the details of the vulnerability without our prior written consent.
3. Access, store, or share any customer or internal data as part of your testing.
4. Access unnecessary, excessive or significant amounts of data.
5. Modify data in the Organisation's systems or services.
6. Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
7. Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
8. Disrupt the Organisation's services or systems.
9. Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with “best practice”, for example missing security headers.
10. Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support or the presence of TLS1.0 support.
11. Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
12. Social engineer, ‘phish’ or physically attack the Organisation's staff or infrastructure.
13. Demand financial compensation in order to disclose any vulnerabilities.

You must:

1. Always comply with data protection rules and must not violate the privacy of Chess users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
2. Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

Legal

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organisation or partner organisations to be in breach of any legal obligations.