CREST WEBSITE: RESPONSIBLE VULNERABILITY DISCLOSURE POLICY

Please read this CREST Disclosure Policy document fully before you report any vulnerabilities on our website. Doing so will help ensure that you understand the policy and comply with it.

1. Background

1.1 CREST is an international not-for-profit, membership body representing the global cyber security industry. Our goal is to build trust in the digital world by raising standards in the global cyber security industry.

1.2 We work closely with the cyber community and as such, accept vulnerability reports from professional security testers on areas of our website to ensure the safety of visitors and to recognise the community's work in continuing to build a safe and secure online environment.

1.3 This Responsible Disclosure Policy reflects our values and acknowledges our legal responsibility to good-faith security researchers that are sharing their expertise. It also reinforces the principles of responsible disclosure that allow time for stakeholders to remediate any genuine vulnerabilities prior to any details being published.

2. Rules of Engagement

i. Provide details of the vulnerability finding. This should include information on the vulnerability, the URL or page where the vulnerability can be observed, and steps to reproduce it to validate the report. Steps should be benign, non-destructive, proof of concept which will allow timely and accurate triage and reduce the likelihood of duplicate reports or malicious exploitation of some vulnerabilities.

ii. Do not attempt to conduct post-exploitation on our website, including modification or destruction of data.

iii. Do not attempt brute force or denial of service attacks.

iv. Do not attempt to target CREST employees and/or customers and/or member companies.

v. Do not threaten or try to extort CREST.

vi. Do not act in bad faith and make ransom requests.

vii. Do not submit reports indicating that a service, for example, does not align with "best practice".

viii. Do not share any data or information you have found with anyone (publicly or privately) other than current CREST employees who have been assigned to your report. Do not hold data longer than required (see 4.4).

Failure to follow these rules may result in legal action.

3. Initial Scope

2.1 Domain in scope: http://www.crest-approved.org

2.2 CREST's Responsible Vulnerability Disclosure Policy does not cover the following:

i. Vulnerabilities affecting users of outdated browsers or platforms.

ii. Account brute force.

iii. Physical or social engineering attacks.

iv. Email spoof.

v. Unverified results of automated tools or scanners.

vi. Content spoofing.

vii. DOS/DDOS.

This Policy was created in October 2022.

viii. "Theoretical" vulnerabilities without any proof or demonstration of the real presence of the vulnerability.

4. Legal Posture

4.1 Security testers must adhere to the applicable legislation of their location and the location of CREST, including Government or Regulatory Bodies. This includes data protection rules.

4.2 Security testers should not disclose vulnerability details to the public. Once your reported vulnerability has been resolved, we request that you co-ordinate with us in advance of any public disclosure in order to unify any guidance to affected users. Please do not demand or expect credit or monetary reward for disclosure, and do not seek or expect to profit (disproportionately) from such disclosure.

4.3 CREST will take action against anything which is deemed to be illegal behaviour or detrimental to CREST's website and any individual's personal data.

4.4 Security testers must securely delete all data retrieved during their research as soon as it is no longer required or within one month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

4.5 This policy does not provide any form of indemnity by CREST or any third party for any actions if you are in breach of the law and/or this policy.

4.6 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 CREST or its partner organisations to be in breach of any legal obligations.

5. How to Submit a Vulnerability Report

5.1 Please submit vulnerability reports via email to security@crest-approved.org.

5.2 If you have difficulty creating a report, there is some useful content online. Please refer to Tips For Creating a Strong Vulnerability Assessment Report | RSI Security or How to write a vulnerability report - Infosec Resources (infosecinstitute.com).

5.3 Please ensure you are including sufficient information for us to verify and evaluate the risk.

6. What to Expect

6.1. Once we have received and read your report, we will contact you within five working days to confirm we are looking into it.

6.2. We will then assess the vulnerability within 10 business days from the date of our acknowledgement (6.1) and prioritise remediation looking at impact, severity, and exploit complexity. We may have further questions which could cause this timeline to be extended.

6.3. We will let you know the outcome of your report.

6.4. Please note the public disclosure provisions at Clause 4.2 above.

6.5. We expect open and positive communication with you, which includes mutual respect and transparency.

We respect the time taken by security testers and in turn request that respect and support is shown to all parties involved.

Thank you for helping keep CREST and our users safe.

This Policy was created in October 2022.