DMI FINANCE

DMI Responsible Disclosure Policy

DMI FINANCE

DMI Finance Responsible Disclosure Policy

At DMI Finance, data security is a top priority. If you believe that you have discovered a potential vulnerability, please report it to cyberdefense@dmifinance.in

We request your assistance in maintaining the security of DMI Finance by reporting any findings responsibly and adhering to this policy.

Reporting security issues

E-mail your findings to cyberdefense@dmifinance.in.Please submit your findings in the following format:

- Description of the issue
- Affected endpoint/URL
- Severity
- Impact
- Proof of concept including step-by-step approach, screenshots/video
- Recommended Solution

What we commit

- Your report will be handled with strict confidentiality, and your personal details will not be shared with third parties without your explicit permission.
- Your report will be responded to within **five business days** with a thorough evaluation.
- As a token of appreciation for your assistance, a certificate of appreciation (in soft copy format) will be awarded to researchers who report valid and high-impact security issues under the following conditions.
    - You must be the first researcher to disclose the bug responsibly. Any duplicates will not be considered.
    - Must strictly adhere to the Responsible disclosure policy.

What we request

- Kindly avoid public disclosure of any security issues unless the DMI Finance Security Team approves it.
- Once you responsibly disclose a vulnerability, please be patient and allow a reasonable amount of time for it to be fixed and for you to be updated.
- Please provide sufficient information to reproduce the vulnerability.

DMI FINANCE

- Please stick to the target mentioned in the scope and refrain from testing any other targets.
- Please use the custom header **X-Security-Test: <Your Userid>** in all test requests to identify your requests. Any requests not following this protocol will be considered malicious. Burp and other proxies allow the easy automatic addition of headers to all outbound requests. Kindly share what header you set so we can identify it easily.
- Please refrain from using scanners or automated tools. Please perform manual testing and refrain from sending multiple requests within a short time frame to our targets.
- Upon discovery of any security vulnerability that may expose sensitive data or grant access to resources, please refrain from modifying any data or configuration.
- Please avoid exploiting the vulnerability or problem you have discovered, for example, by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data.
- Please avoid attacks on physical security, social engineering, distributed denial-of-service attacks, spam, or applications from third parties.

Targets

- DMI FINANCE and this group of companies' websites
- DMI HFC Rapid app and application
- API connecting DMI Finance

In-scope vulnerabilities

- Remote Code Execution
- Authentication Bypass
- Privilege Escalation
- Privacy/Sensitive Information Disclosure
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- Injection Issues (SQLi, XML, LDAP, etc.)
- Session-Related Issues (Session fixation, session hijack, etc.)
- Open Redirects with a significant security impact
- Cross-Origin Resource Sharing with significant security impact
- Remote / Local File Inclusion
- Malicious use of functionality
- API Abuse
- Infrastructure-related issues (server issues, etc.)
- Other high-impact issues

DMI FINANCE

Out-of-scope vulnerabilities

Issues that have little or no impact do not qualify for our program.

- Bypassing root/jailbroken detection
- SSL Pinning Bypass
- Vulnerabilities in 3rd party applications/libraries / APIs
- Clickjacking / Tapjacking
- DOS/DDOS Attacks
- Self XSS
- Version Disclosure
- Error messages with no sensitive data
- Third-party API key disclosures without any impact or those that are supposed to be open/public.
- Missing HTTP Security Headers (e.g. HSTS)
- Know public files or directories disclosure (e.g. robots.txt, CSS/images, etc.)
- Brute force Attacks / Account lockouts / Rate limit bypasses without high impact
- Login - Logout cross-site request forgery
- CSV / HTML / Text Injection
- Social engineering (Phishing) / Spamming (e.g. SMS/Email Bombing)
- Screen bypass
- Forced Browsing
- Certificate-related issues (e.g. Weak Cyphers, etc.)
- DNS issues (e.g. DMARC, DKIM, SPF records, etc.)
- Vulnerabilities that require physical device access (e.g. USB debugging), root/jailbroken access or third-party app installation to exploit the vulnerability
- Reporting usage of known-vulnerable software/known CVEs without proving the exploitability

Contact: cyberdefense@dmifinance.in
Acknowledgements:
Preferred Languages: English