Responsible Vulnerability Disclosure Program

Document Control

Document Number	DR/IT/00239
Current Version	1.0
Last Updated	21-Jun-2021
First Published	12-Jun-2021
Document Owner	Ahmad
Classification	Private
Approved By	Jimmy Mistry
Review Due Date	12-Dec-2021

Table of Contents

Purpose

Della Group is committed to ensuring the safety and security of our products, services, and customers. As such, we are publishing this Policy and Program.

Program Overview

By introducing a RVDP, Della Group is aiming to leverage the skills of security personnel available world-wide to increase their security posture.

Scope

In-Scope

The following assets are in the scope of the RVDP program:

Websites

- dellaresorts.com

Out-of-Scope

The following assets are out of scope:

- Digital asset of any consultants, clients, vendors, guests and users of Della Group.
- Disruption of service using attacks like DDoS.
- Physical attack on any infrastructure hosting any digital assets or services.
- Office infrastructures used by any of the Della Group company.
- Phishing / Vishing or any other social engineering attack on employees, consultants, clients, vendors, guests and users.

Third-Party Services

Some components and services of Della Group digital assets are either hosted or operated by our vendors or partners (e.g., route53, Auth0). We can't authorize you to test such components and services on behalf of the owners and will not reward any such reports. If you are unsure whether a domain is in-scope or not please reach out to us.

Della group cannot be held responsible for any legal action arising from testing such services.

Vulnerability Disclosure Philosophy

The intent of this policy is to provide guidance regarding the process involved around submitting a vulnerability disclosure program. This program is based on good faith practices and Finder and Security Team have their share of responsibility.

Finder's responsibilities

Respect the rules: Operate within the rules set forth here or discuss with us if in strong disagreement with the rules.

Respect privacy: Make a good faith effort not to access or destroy another user's data or cause service disruption.

Be patient: Make a good faith effort to clarify and support their reports upon request.

Do no harm: Act for the common good through the prompt reporting of all found vulnerabilities. Never willfully exploit without permission.

Security team responsibilities

Prioritize security: Make a good faith effort to resolve reported security issues in a prompt and transparent manner.

Communicate: Make sure to communicate with Finder in timely manner to work together in fixing the security vulnerability

Respect Finders: Give finders public recognition for their contributions by all possible ways (e.g., bug bounty hall of fame).

Reward Finder: Appropriately incentivize security research carried out by Finder to acknowledge the effort and skill demonstrated.

Program Maintenance

Supporting standards, guidelines and procedures will be issued on an on-going basis by Della Group. Subsequent changes or updated versions of such standards, guidelines and procedures shall be notified via e-mail or other relevant communication mode such as dedicated webpage on the website(s).

Safe Harbor

Dell Group will not engage in legal action against individuals who, in good faith, submit vulnerability reports following these guidelines and procedures.

Program Details

How to submit a Vulnerability?

First, Finder should review and agree to the Responsible Disclosure Agreement. Then, submit the vulnerability report to security@dellagroup.in. Finder should provide all details in the submission report to avoid undesirable delays. Provide clear, concise reproduction steps or a proof-of-concept.

Vulnerability Review Process

Upon receipt of the report, security team will review and investigate the vulnerability as soon as practicable and provide remediation no later than within 30 days from receipt of the report. Finder will be notified when this investigation starts.

Contents of the report will be made available to the security team and will remain private to allow them sufficient time to publish a remediation.

Following activities will occur as part of the review process (not in sequence):

- Identification of issues.
- Impact Assessment.
- Solution design, development, testing and deployment.
- Involvement of law enforcement, forensics (if needed).
- Notifications for affected stakeholders (if needed).

If assessments determine that the vulnerability requires remediation, we will start remediating the vulnerability as soon as practicable.

Vulnerability Scoring Mechanism

We use CVSS 3.0 (Common Vulnerability Scoring Standard) to calculate severity.

Vulnerability Report Requirements

For a submission report to be considered for remediation (and potentially reward program) must include the following:

- Full description of the vulnerability being reported, including the exploitability and impact.
- Steps to replicate.
- Supporting evidence such as:
    - Screenshots.
    - Traffic logs.
    - Web/API requests and responses.
    - IP address used for testing.
    - Email address or user ID of any test accounts.

Vulnerability Public Disclosure Request

After the Report has been closed, public disclosure may be requested by either the Finder or the Security Team.

Default: If neither party raises a request, the contents of the Report will NOT be made public.

Mutual agreement: We encourage the Finder and Security Team members to remain in open communication regarding disclosure timelines. If both parties agree, the contents of the Report can be made public on a mutually agreed timeline.

Protective disclosure: If the Security Team has evidence of active exploitation or imminent public harm, they may immediately provide remediation details to the public so that users can take protective action.

Extension: Due to complexity and other factors, some vulnerabilities will require longer than the default 30 days to remediate. In these cases, the Report may remain non-public to ensure the Security Team has an adequate amount of time to address a security issue. We encourage Security Teams to remain in open communication with the Finder when these cases occur.

Last resort: If 180 days have elapsed with the Security Team being unable or unwilling to provide a vulnerability disclosure timeline, the contents of the Report may be publicly disclosed by the Finder. We believe transparency is in the public's best interest in these extreme cases.

Public Recognition

Following the successful fix of the vulnerability, security team will disclose the vulnerability and the successful remediation on our website, subject to the terms and conditions of the Responsible Disclosure Agreement. If you prefer to be credited by name, please let us know in email.

The finder will be credited if:

- They are the first person to file a Report for a particular vulnerability.
- The vulnerability is confirmed to be a valid security issue.
- They have complied with these guidelines.

If the finder wishes to remain anonymous, then are free to either use a pseudonym or decline from being mentioned.

Security team will need written consent from the finder regarding anonymity or public recognition.

Bounty Program

After remediation, Finder may be eligible to receive a bounty payment, subject to the terms and conditions of the Responsible Disclosure Agreement. While we use CVSS 3.0 (Common Vulnerability Scoring Standard) to calculate severity, we reserve the right, in our sole discretion, whether the vulnerability qualifies for a bounty payment.

Dell Group Responsible Disclosure program DOES NOT offer monetary rewards outside of this program on any platform.

Eligibility

We are aware that some Security Teams may offer monetary rewards for vulnerability disclosure. The decision to grant a reward is entirely at Della Group's discretion. The amount of each bounty payment will be determined by the Security Team. Bounty payments are subject to the following eligibility requirements:

- We cannot pay bounties to residents or those who report vulnerabilities from a country against which the country has trade restrictions or export sanctions as determined by the Govt. of India
- Minors are requested not to participate in the program. We love and encourage sharp technical skills of kids. However, due to various legal restrictions we'd request you to not participate.
- All payments will be made in either U.S. dollars (USD) or Indian Rupees (INR) and will comply with local laws, regulations, and ethics rules. You are responsible for the tax consequences of any bounty you receive, as determined by the laws of your country.

- It is your sole responsibility to comply with any policies your employer may have that would affect your eligibility to participate in this bounty program.

Information Protection

Certain personally identifiable information (PII) will be collected as part of the report submission process. This information will be stored, processed, protected, and archived in line with corporate data privacy and protection guidelines. Data will be encrypted as per corporate encryption guidelines.

Finder's data and submission report data will be known only to the Security team and will be used only for product/service improvement and patching of security vulnerabilities. Data gathered cannot be used for other purposes such as product/service cross-selling, marketing purposes.

Under exceptional circumstances, sharing with law enforcement is possible.

Private Bug Bounty Program Participation

If the Finder decides to participate in private bug bounty programs not associated with Della Group, they are doing so at their own risk. Special concessions such as Della Group bug bounty, and legal protection via safe harbor will not be afforded to such Finders. Review the policies and procedures for such programs carefully before participation.

Della Group will not hesitate to initiate legal action against the finder if vulnerabilities discovered via such private programs are published for public consumption.

Terminology

Security Team: A team of individuals who are responsible for addressing security issues found in a product or service. Depending on the circumstances, this might be a formal security team from an organization, a group of volunteers on an open-source project, or an independent panel of volunteers (such as the Internet Bug Bounty).

Finder: Also known as white hat hackers. Anyone who has investigated a potential security issue in some form of technology, including academic security researchers, software engineers, system administrators, and even casual technologists.

Report: A Finder's description of a potential security vulnerability in a particular product or service. Reports always start out as non-public submissions to the Security Team.

Vulnerability: A software bug that would allow an attacker to perform an action in violation of an expressed security policy. A bug that enables escalated access or privilege is a vulnerability. Design flaws and failures to adhere to security best practices may qualify as vulnerabilities. Weaknesses exploited by viruses, malicious code, and social engineering are not considered vulnerabilities unless the Security Team says otherwise in the program's policy.

Programs: Security Teams may publish a Program and Program Policy designed to guide security research into a particular service or product. If this program is private, your participation is entirely optional and subject to non-disclosure by default.

Compliance Measurement

The Information Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Enforcement

Any finder found to have violated this program may be subject to retraction of disqualification from the bug bounty program, and/or potential legal action.

Exceptions to Policy

Unless specifically approved, any deviation from this program is prohibited. Any deviation to or non-compliance with this policy shall be reported to the Information Security team and the Chief Information Security Officer (CISO).

All exceptions to this program must be approved by CISO.