Bug & Vulnerability Reporting

Please review these Bug Bounty Program Terms before submitting a report. By submitting your report, you agree to the terms of the Bug Bounty Program.

If you follow the program terms, we will not initiate a lawsuit or law enforcement investigation against you in response to your report. Please understand that this waiver does not apply to your security research that involves the networks, systems, information, applications, devices, products, or services of another party (which is not OpenGrants). We cannot and do not authorize security research in the name of other entities.

Important: To report a potential security issue or vulnerability with the OpenGrants platform or app, submit a bug report using the purple feedback tab to the right of the scree.

In the report please include the following information:

- The name(s) of the OpenGrants product or technology and the respective version information.
- Detailed description of the potential security vulnerability.
- Proof-of-concept that details the reproduction of the potential security vulnerability.
- The more details provided in the initial report, the easier it will be for OpenGrants to evaluate your report.

Security Researcher and Reporter Eligibility Criteria

All criteria must be met in order to participate in the Bug Bounty Program.

- You are reporting in your individual capacity or, if you are employed by a company or other entity and are reporting on behalf of your employer, you have your employer's written approval to submit a report to the OpenGrants® Bug Bounty Program.
- You are at least 18 years of age, and, if considered a minor in your place of residence, you have your parent's or legal guardian's permission prior to reporting.
- You are not a resident of a U.S. Government embargoed country.
- You are not on a U.S. Government list of sanctioned individuals.
- You are not currently nor have been an employee of Egeria Corporation dba OpenGrants, or an OpenGrants subsidiary, within 6 months prior to submitting a report.
- You are not currently nor have been under contract to Egeria Corporation dba OpenGrants, or an OpenGrants subsidiary, within 6 months prior to submitting a report.
- You are neither a family nor household member of any individual who currently or within the past 6 months meets or met the criteria listed in the two bullet points directly above.
- You agree to participate in testing mitigation effectiveness and coordinating disclosure/release/publication of your finding with OpenGrants.
- You did not and will not access any personal information that is not your own, including by exploiting the vulnerability.
- You did not and will not violate any applicable law or regulation, including laws prohibiting unauthorized access to information. To clarify, OpenGrants does not view testing that is done in compliance with the terms and conditions of this bug bounty program as unauthorized.
- There may be additional restrictions on your eligibility to participate in the bug bounty depending upon your local laws.
- If at any point while researching a vulnerability, you are unsure whether you should continue, immediately send a message to OpenGrants (security@OpenGrants.io).

Sensitive and Personal Information

- Never attempt to access anyone else's data or personal information including by exploiting a vulnerability. Such activity is unauthorized. If during your testing you interacted with or obtained access to data or personal information of others, you must:
- Stop your testing immediately and cease any activity that involves the data or personal information or the vulnerability.
- Do not save, copy, store, transfer, disclose, or otherwise retain the data or personal information.
- Alert OpenGrants immediately and support our investigation and mitigation efforts.

Failure to comply with any of the above will immediately disqualify any report from bounty award eligibility.

Eligible Reports (in scope)

To be eligible for bounty award consideration, your report must meet the following requirements:

- The OpenGrants products in your report correspond to an item explicitly listed below as "Eligible OpenGrants branded products and technologies".
- The vulnerability you identify must be original, not previously reported to OpenGrants, and not publicly disclosed.
- The report must show that the potential vulnerability has been demonstrated against the most recent publicly available version of the affected product or technology.

The report must contain clear documentation that provides the following:

- An overview/summary of the reported vulnerability and potential impact.
- Detailed explanation of the reported vulnerability, how it can be exploited, the impact of the vulnerability being successfully exploited and likelihood of a successful exploit.
- The name and specific version of the OpenGrants product(s) the potential vulnerability is reported on.
- Proof of Concept (POC) code or instructions that clearly demonstrates an exploit of the reported vulnerability. The POC must include instructions that if followed by the OpenGrantsproduct engineering team would successfully demonstrate existence of and exploitability of the vulnerability.
- Information on how any Proof of Concept (POC) code was developed and compiled. If appropriate, include the description of the development environment, including the compiler name, compiler version, options used to compile, and operating system revisions.

Eligible OpenGrants branded products and technologies that are maintained and distributed by OpenGrants:

- OpenGrants platform at portal.opengrants.io
- OpenGrants Mobile App

OpenGrants, at its sole discretion, may reject any submission that we determine does not meet these criteria above or that are deemed as ineligible as set forth below.

Ineligible Reports (out of scope)

The following are general categories of vulnerabilities that are considered ineligible for a bounty award:

- Vulnerabilities in pre-release product versions (e.g., Beta, Release Candidate).
- Vulnerabilities in product versions that are no longer under active support.
- Vulnerabilities already known to OpenGrants. However, if you are the first external security researcher to identify and report a previously known vulnerability, you may still be eligible for a bounty award.
- Vulnerabilities present in any component of an OpenGrants product where the root-cause vulnerability in the component has already been identified for another OpenGrants product.
- Vulnerabilities in products and technologies that are not listed as "Eligible OpenGrants branded products and technologies", including vulnerabilities considered out of scope as defined below.

Any conduct by a security researcher or reporter that appears to be unlawful, malicious, or criminal in nature will immediately disqualify any submission from the program. Do not engage in extortion.

Bug Bounty Awards

Eligibility for any bug bounty award and award amount determinations are made at OpenGrants's sole discretion. These are some general guidelines that may vary from published documentation:

Awards may be greater:

- based on the potential impact of the security vulnerability
- for well-written reports with complete reproduction instructions / proof-of-concept (PoC) material. See the eligible report requirements above.
- if a functional mitigation or fix is proposed along with the reported vulnerability.

OpenGrants will award a bounty award for the first eligible report of a security vulnerability.

Awards are limited to one (1) bounty award per eligible root-cause vulnerability.

OpenGrants will award a bounty in $GRANT depending on the vulnerability type and originality, quality, and content of the report. **Please educate yourself on $GRANT as its not a crypto currency but represents equity ownership in OpenGrants.** You can learn more here.

OpenGrants will publicly recognize awarded security researchers via OpenGrants Security Advisories at or after the time of public disclosure of the vulnerability, in coordination with the security researcher who reported the vulnerability.

Award amounts may change with time. Past rewards do not necessarily guarantee the same reward in the future.

Bounty Award Schedule

Each bug bounty report is individually evaluated based on the technical details provided in the report. OpenGrants generally follows the processes below to evaluate and determine the severity of a reported potential security vulnerability.

Triage – A team of OpenGrants product engineers and security experts will determine if a vulnerability is valid and an eligible OpenGrants product or technology is impacted.

Vulnerability severity determination – OpenGrants product security engineers and OpenGrants security experts work to determine the severity and impact of a vulnerability.

We take into consideration a range of factors when determining the award amount for eligible reports. Those factors include, but are not limited to, the quality of the report, impact of the potential vulnerability, CVSS severity score, whether a POC was provided and the quality of the POC, type of vulnerability.

Bounty Award Payment

Bounty award arrangements under this program, including but not limited to the timing, bounty amount and form of payments, are at OpenGrants's sole discretion and will be made on a case-by-case basis.

OpenGrants makes no representations regarding the tax consequences of the payments OpenGrants makes under this program. Participants in this program are responsible for any tax liability associated with bounty award payments.

OpenGrants Intellectual Property

By submitting your content to OpenGrants(your "Submission"), you agree that OpenGrants may take all steps needed to validate, mitigate, and disclose the vulnerability, and that you grant OpenGrants any and all rights to your Submission needed to do so.

Specific Examples of Out of Scope Findings

- OpenGrants's web infrastructure, i.e., website domains owned and/or operated by OpenGrants, are out of scope. Please send security vulnerability reports against OpenGrants.io and/or related web presence to security@opengrants.io
- OpenGrants products intended for prototyping use or that are "open" in order to provide customers with debugging capability are out of scope.
- OpenGrants freeware applications are out of scope.

In Scope eligible products and technologies are listed above, if you are unsure whether a product or technology is eligible, contact OpenGrants at security@opengrants.io

OpenGrants reserves the right to alter the terms and conditions of this program at its sole discretion.

May 23rd, 2024

Share This Story, Choose Your Platform!

LEARN MORE

- About Us
- Pricing
- Perks
- Legal
- Sitemaps
- Learn About Grants

WORK WITH OPENGRANTS

- Be a Freelance Grant Writer
- Invest in OpenGrants
- API
- OpenGrants Data
- Professional Services
- Knowledge Base

FOLLOW US

- Newsletter
- Blog
- Attend Our Events
- Twitter
- LinkedIn
- YouTube

HOW WE'RE DIFFERENT

- OpenGrants versus Grants.gov
- OpenGrants versus Grant Station
- OpenGrants versus Foundation Center
- OpenGrants versus Instrumentl
- OpenGrants versus Upwork