Grid Dynamics

Responsible Disclosure Policy

Introduction

Maintaining confidentiality, integrity, and availability of Grid Dynamics information, data, services, systems, and networks is essential and a top priority for Grid Dynamics. We encourage our users and members of the security community to report possible vulnerabilities and incidents privately and responsibly so that we can address these issues quickly.

This policy sets out the processes to report to Grid Dynamics any incident, suspicion of an incident, or a vulnerability found on any externally exposed Grid Dynamics systems. An incident involves the loss of, unauthorized access to, or unauthorized disclosure of, sensitive information. A vulnerability is any technical flaw that can be found on a system that could lead to an incident or to an interruption of the provided service.

This policy applies to any and all incidents and vulnerabilities you are considering reporting to us. We recommend reading this policy fully before you report an incident or vulnerability and always acting in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer monetary rewards for vulnerability disclosures, and do not run a bug bounty program at the moment.

Reporting

If you believe you have found an incident or a security vulnerability, please submit your report to us using abuse@griddynamics.com Any reports regarding personal data privacy issues and privacy regulations, GDPR and CCPA included, should be submitted to dpo@griddynamics.com instead.

In your report please include details of:

- The website, IP, page, application, library, or network service where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example; “XSS vulnerability”.
- Exact steps to reproduce. These should be a benign, non-destructive, proof of concept.
- URL and parameters demonstrating the vulnerability (if applicable).
- Any relevant details of your system’s configuration.
- Your IP address, to match with our logs.
- Please do not send any executable attachments.

If you want to report an online leak of sensitive Grid Dynamics information, please provide a working reference link to it or, if not applicable, a sample of the sensitive information exposed and how you have discovered it.

If you have found a lost Grid Dynamics-owned laptop or other device, please include its make, serial number, and where the device was discovered.

This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as subdomain takeovers.

What to expect

After you have submitted your report, we will respond to your report within 5 working days and aim to triage your report within 10 working days.

We’ll also aim to keep you informed of our progress. Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. Our goal is to address reported, legitimate issues as quickly and as efficiently as possible, however handling disclosed issues may not be easy or straightforward. While some issues can be analyzed and resolved quickly, others may be more complex or

have a broader impact that requires more careful work. You are welcome to inquire about the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation and ensure users are safe and protected. If we can, we will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users and ensure any remediation is fully rolled out before public disclosure, so please do continue to coordinate any public release with us.

Guidance

You must NOT:

- Break any applicable cybercrime laws or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in Grid Dynamics's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt or deliberately attempt to interrupt or degrade Grid Dynamics's services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practices", for example missing HTTP security headers or TRACE/TRACK web methods being used.
- Submit reports detailing TLS configuration weaknesses, for example "weak" cipher suite support or the presence of TLS1.0 support.
- Communicate any vulnerabilities or associated details other than by means described in this policy.
- Social engineer (phish, smish, spoof, or otherwise maliciously impersonate) or physically attack (lockpick, tailgate, etc.) Grid Dynamics's staff and/or infrastructure.
- Break into/root/backdoor a lost Grid Dynamics device.
- Demand financial compensation in order to disclose any vulnerabilities.

You must:

- Always comply with data protection rules and avoid violating the privacy of Grid Dynamics's users, staff, contractors, customers, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from our systems or services.
- Securely delete (see NIST 800-88 for reference) all data retrieved from us 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 applicable data protection laws).

Legalities

This policy is designed to be compatible with good industry practices on responsible incident reporting and vulnerability disclosure. It does not give you permission to act in any manner that is inconsistent with cybercrime or privacy/data protection laws, or which might cause the Grid Dynamics, its affiliates, customers, or partners to be in breach of any legal obligations and/or privacy regulations. and