Vulnerability Disclosure Policy

Purpose

The purpose of this document is to establish the policy for reporting security vulnerabilities of OwnBackup owned and managed assets. This policy provides security researchers guidelines to conduct ethical research and collaboration of discovered security vulnerabilities of OwnBackup.

Program Rules

- Notify us as soon as you discover a potential security vulnerability.
- Only use or access accounts and information that belong to you.
- Do not destroy or modify data that is not yours.
- Do not degrade the performance of OwnBackup products and services or our users.
- Do not perform social engineering, physical, or denial of service attacks on OwnBackup personnel, locations, or assets.
- This policy applies to OwnBackup's products, services, and systems. Always be careful to verify whose assets you are testing while performing research.
- Vulnerabilities found in vendor systems or third party services not managed by OwnBackup fall outside of this policy's scope and should be reported directly to the vendor via their disclosure programs.
- Do not perform automated scans or tests on OwnBackup systems or networks. OwnBackup performs such scans and tests itself.
- This policy is not an invitation to proactively scan our systems or networks for vulnerabilities. Scans that put an excessive load on OwnBackup's systems or resources may result in investigation and legal action.
- If you aren't sure if a system is in scope or need help reporting a finding to a vendor, contact us at ownbackup.vdp@ownbackup.com We're happy to help!

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct, and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Out of Scope Vulnerabilities

- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working proof of concept.
- Clickjacking on pages with no sensitive actions.
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions.

- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Accessing, or attempting to access, data or information that does not belong to you
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you.
- Conducting any kind of physical or electronic attack on OwnBackup personnel, property, or data centers.
- Defacement.
- Social engineering any OwnBackup service desk, employee or contractor.
- Violating any laws or breaching any agreements in order to discover vulnerabilities.
- Performing actions that may negatively affect OwnBackup or its users (e.g. Spam, Brute Force, Denial of Service…)
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS.
- Rate limiting or bruteforce issues on non-authentication endpoints.
- Missing best practices in Content Security Policy.
- Missing HttpOnly or secure flags on cookies.
- Missing email best practices (invalid, incomplete or missing SPF/DKIM/DMARC records, etc.).
- Vulnerabilities only affecting users of outdated or unpatched browsers (less than two stable versions behind the latest released stable version).
- Software version disclosure / banner identification issues / descriptive error messages or headers (e.g., stack traces, application or server errors).
- Public zero-day vulnerabilities that have had an official patch for less than 1 month will be awarded on a case by case basis.
- Tabnabbing or similar impersonation attacks.
- Open redirect — unless an additional security impact can be demonstrated.

How to Report a Vulnerability

We accept and communicate about potential security vulnerability reports via ownbackup.vdp@ownbackup.com.

We will acknowledge receipt of your report within three business days.

What we would like to see from you
To help us triage and remediate potential findings, a good vulnerability report should:

- Describe the vulnerability, precisely where it was discovered, and the real-world impact.
- Reports from automated scanning tools are not accepted.
- Offer a detailed description of the steps needed to reproduce the vulnerability (POCs, screenshots, and videos are helpful).
- Please include one vulnerability per report (unless in an attack chain).

- Don’t report automated scanner results without proof of exploitability.

The OwnBackup security team commitment:

We ask that you do not share or publicize an unresolved vulnerability with/to third parties. If you responsibly submit a vulnerability report, the OwnBackup security team and associated development organizations will use reasonable efforts to:

- Respond in a timely manner, acknowledging receipt of your vulnerability report.
- Provide an estimated time frame for addressing the vulnerability report.
- Notify you when the vulnerability has been fixed.

We are happy to thank every individual researcher who submits a vulnerability report helping us improve our overall security posture at OwnBackup.