Responsible Disclosure Policy

bynder

Public

At Bynder, we are committed to keeping our systems, network and product(s) secure. Despite the measures we take, the presence of vulnerabilities will always be possible. When such vulnerabilities are found, we'd like to learn of them as soon as possible, allowing us to take swift action to shore up our security.

Under Bynder's Responsible Disclosure Policy, you are allowed to search for vulnerabilities, **so long as you don't**:

- execute or attempt to execute a Denial of Service (DoS)
- make changes to a system
- install malware of any kind
- social engineer our personnel or customers (including phishing)
- scan or run tests in a manner that would degrade the operation of the service or negatively affect our customers in any way
- physically attack or damage Bynder property, offices or data centers or attempt to do so
- run tests on third party applications, websites or services that integrate with or link to Bynder
- scan or attack the Amazon Web Services infrastructure or attempt to do so

Breaching the above restrictions may result in Bynder launching an investigation and/ or taking legal action to the greatest extent of Bynder's legal obligation and rights or that of our partners and customers.

If you do discover a vulnerability, please contact us as soon as possible by sending an (encrypted) email to security@bynder.com. To prevent information falling into the wrong hands, please use the following public key: *(insert public key box here as on bynder.com/en/security)*

What we ask of you:

- Submit your vulnerability report as soon as possible after discovery
- Do not abuse or exploit discovered vulnerabilities in any way for any purpose
- Do not share discovered vulnerabilities with any entities or persons other than Bynder and its employees until after Bynder has confirmed the vulnerability has been resolved
- Provide us with adequate information to enable us to investigate the vulnerability properly (to be able to investigate properly, we will need to be able to efficiently reproduce your steps)
- Provide us with information required to contact you (at least telephone number or email address)

What we promise:

- We will respond to your report within 5 business days of receipt, with our evaluation of the report and an expected resolution date.
- We will keep you regularly informed of our progress toward resolving the vulnerability.
- If you have followed the above instructions, we will not take any legal action against you regarding the report.

Rewards and attribution:

- Please do not ask for a reward before sharing the vulnerability, as we need to evaluate your report before responding.
- If you report a vulnerability that is unknown to us, and if you are not from a country where we are prohibited by law from making payments (e.g. due to sanctions), we may decide to offer you a reward based upon our assessment of the criticality of the vulnerability.

Assets in scope:

- https://www.bynder.com
- https://wave-trial.getbynder.com

Accounts can be self provisioned at https://www.bynder.com/en/trial.

Out of scope assets:

- *.bynder.com
- *.getbynder.com
- *.webdamdb.com
- *.webdam.com

Acquisitions:

For all our acquisitions, in order to give our development and security teams time for internal review and remediation, we will introduce a six-month blackout period. Vulnerabilities reported in that period will not qualify for a reward.

Out of scope vulnerabilities:

- Vulnerabilities affecting users of outdated or unsupported browsers or platforms
- Password and account recovery policies, such as reset link expiration or password complexity
- Issues that require unlikely user interaction
- Attacks requiring MITM or physical access to a user's device
- Attacks that require prior access to a user's email account
- Reports from automated tools or scanners
- Clickjacking/UI Redressing
- Reflected file download
- Verbose error pages (without proof of exploitability)
- SSL/TLS Best Practices
- Incomplete/Missing SPF/DKIM
- Fingerprinting / banner disclosure on common/public services
- Disclosure of known public files or directories, (e.g. robots.txt)
- Content spoofing (text injection)
- Tabnabbing
- OPTIONS HTTP method enabled
- Recently disclosed zero-day vulnerabilities that had an official patch for less than 30 days will be awarded on a case by case basis
- Presence of autocomplete attribute on web forms

- Use of a known-vulnerable library (without proof of exploitability)
- CSV Injection
- Missing HTTP Security Headers (without proof of exploitability)
- "Self" Cross-Site Scripting (unless if it is part of a chain)
- Missing cookie flags
- Missing best practises in Content Security Policy

The following template can be used when submitting a vulnerability:

```
# Description
[Description of the identified vulnerability]

# Steps to reproduce
1. Step 1
2. Step 2
[...]

# Impact
[What could an attacker achieve by exploiting the
vulnerability]
```

Any report submitted in relation to this Responsible Disclosure Policy will be handled with great care with regards to the privacy of the reporter. We will not share your personal information with third parties without your permission, unless we are legally required to do so.

About Bynder

Bynder is a leading cloud-based branding automation and marketing solution that removes the roadblocks to creativity and empowers marketers to easily create, organize and share digital content.

Founded in 2010, Bynder has been on a mission to make marketing more agile. Streamlining the content production process for marketers globally, users can collaborate from anywhere in the world, at any time via one centralized platform. Supporting end-to-end brand consistency, with the click of a button, you can resize graphics and videos, distribute files that are customized for social and digital channels, and prove and improve your marketing ROI. Helping organizations to reduce the time to market of all marketing materials, Bynder grew into the initiative solution it is today.

Named a Deloitte Fast 50 Rising Star in 2015, Bynder is driven by action and thought leadership. Powering digital content management for over 350 companies globally, Bynder is headquartered in Amsterdam but also has regional offices in London, Rotterdam, Barcelona, Boston, and Dubai.

www.bynder.com