Responsible Disclosure Policy

+31 520 21 6226 support@hypernode.com Ertskade 109, 1019 BB, Amsterdam

Responsible Disclosure Policy

We take the security of our systems and our users very seriously, and we value the security community. The responsible disclosure of security vulnerabilities helps us ensure the security and privacy of our users.

Guidelines

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing.
- Use the identified communication channels to report vulnerability information to us.
- Keep information about any vulnerabilities you've discovered confidential between yourself and Hypernode until we've had 90 days to resolve the issue.
- Do not abuse found vulnerabilities. Don't download more information than is necessary to show the vulnerability.
- Do not change or remove data. This includes scrubbing your own 'footprints', logfiles, tmpfiles, history files, etc, etc.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission);
- Keep you updated on our efforts in solving the issue;
- If you are the first to report the issue and we make a code or configuration change based on the issue, we will include you in our Security Hall of Fame.

Scope

We accept reports for vulnerabilities in any of the following:

- All systems and services running under the hypernode.nl, hypernode.com and magereport.com domains, and any of its subdomains.
- All systems and services running in the 194.150.225.0/25 ip range.
- Any published code on our ByteInternet GitHub, Hypernode GitHub, hn-support GitHub gists, or in our documentation.
- Any vulnerabilities on our clusterhosting environment, on the Hypernode vagrant / docker setup, or generic Hypernode vulnerabilities, are also welcome.

Out of scope

In the interest of the safety of our users, staff, the Internet at large and you as a security researcher, the following test types are excluded from scope.

- The testing of sites we host for our customers, including sites hosted under the testbyte.nl, or the hypernode.io domain, is explicitly NOT ALLOWED.
- Any tests on services hosted by 3rd party providers and services, even if hosted under an in-scope domain name.
- Physical testing such as office access (e.g. open doors, tailgating).
- Social Engineering (e.g. phishing, vishing).
- Tests on any applications or systems not listed in the 'Scope' section.
- Testing for UI and UX bugs and spelling mistakes.
- Network level Denial of Service (DoS/DDoS) vulnerabilities or brute force attacks.

Things we do not wish to receive from you are the following:

- Personally identifiable information (PII)
- Credit Card holder data

How to report a security vulnerability

If you believe you've found a security vulnerability in one of our products or platforms please send it to us by emailing security@hypernode.com. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us)
- If you saw any customer data, or confidential information, during your research, please inform us of this as well.
- Your name/handle and a link for recognition in our Hall of Fame.

If you'd like to encrypt the information, please use our PGP-key: (ID: **9AD3B600**, Fingerprint: **0DDE A4A1 50C5 B642 1EBB 1F5B FDE7 0F88 9AD3 B600**)