Vivun Responsible Vulnerability Disclosure Program

Vivun's Philosophy

Protecting customer data has been, and always will be, our top priority at Vivun.

Vivun values the work done by security researchers in improving the security of our products and service offerings. As a result, Vivun encourages the responsible reporting of any scoped or identified vulnerabilities that may be found in our websites. Vivun is committed to working with security researchers to verify, reproduce, and respond to potential vulnerabilities that are reported in accordance with the below requirements. If this policy and Vivun's procedures are followed, Vivun will endeavor to refrain from commencing legal action against researchers for penetrating or attempting to penetrate our systems, provided that the following conditions listed below are met.

Note: The Vulnerability Disclosure Program is strictly voluntary and Vivun will provide no reward or any financial remuneration, including a 'bug bounty,' for any vulnerabilities discovered and reported to Vivun. Further, all activities engaged in by any researcher must be:

1. Legal
2. Not likely to create harm to Vivun, its customers, its users, or any third party
3. In compliance with the Vivun Privacy Policy

Vivun's Requirements for Testing Vivun Systems

Please review these terms before you take any action to test a Vivun system. While we encourage researchers to report to us any vulnerabilities discovered in a responsible manner, Vivun does have rules for engagement pertaining to those assets and means of testing which are in the scope of this policy. Targeting any item not explicitly indicated as an 'In-Scope Asset' or engaging in any activity which is not indicated herein as an 'In-Scope' can and may result in civil litigation or criminal action.

In-Scope Assets

The following is a list of assets for which Vivun is explicitly permitting and encouraging good-faith security research:

- www.vivun.com
- execalliance.vivun.com
- unxpctd.vivun.com
- IT Services:
- - Email
   - DNS

Out of Scope Assets

The following is a list of assets for which Vivun is explicitly excluding and prohibiting from any security research:

- app.vivun.com
- app.eval.vivun.com
- app.revel.vivun.com

In-Scope Activities

The following is a list of activities for which Vivun is explicitly permitting and encouraging good-faith security research:

- Testing should be limited to in scope sites and services that Vivun directly operates. We will not accept reports for third-party services or providers that integrate with Vivun.
- Reporting vulnerabilities with no conditions, demands, or ransom threats.
- Making a good-faith effort to avoid privacy violations and disruptions to others, including (but not limited to) unauthorized access to or destruction of data.

Out of Scope Activities

The following is a list of activities for which Vivun is explicitly excluding and prohibiting from any security

research:

- Sharing, disclosing or publicizing an unresolved vulnerability with or to third parties.
- Performing actions that may negatively affect Vivun or its clients or otherwise impact service availability, including spam, brute force, and/or denial of service.
- Accessing, or attempting to access, data or information that does not belong to you.
- Testing of participating services using anything other than test accounts.
- 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 Vivun personnel, property, or data centers.
- Social engineering any Vivun customer, service desk, employee, or contractor.
- Violating any laws or breaching any Vivun Service Agreements in order to discover vulnerabilities.

Vivun's Commitment to Researchers:

If you responsibly submit a vulnerability report, Vivun will use reasonable efforts to:

- Respond in a reasonable time frame confirming that we received your report.
- Provide an estimated time frame for addressing the vulnerability report.
- Notify you when the vulnerability has been fixed.

Reporting a potential security vulnerability:

- We expect you to privately share details of the suspected vulnerability with Vivun by sending an email to vulnerability-reporting@vivun.com. By sending an email to this address you confirm that you are meeting Vivun's requirements of the Vivun Responsible Disclosure Program, as listed above.
- Provide full details of the suspected vulnerability so the Vivun security team may validate and reproduce the issue – please be sure to include as much detail as possible.
- For any legal questions or concerns, please contact us at Legal@vivun.com.

Legal Terms

Acceptance of Non-Disclosure Terms: All information relating to vulnerabilities that you become aware of through Vivun's Vulnerability Disclosure program is considered Confidential and therefore, you agree that you will not publish or otherwise disseminate publicly (or to any third party) any identified vulnerabilities so as to permit Vivun to effectively remediate the same, without first obtaining written consent from Vivun. For the purposes of obtaining consent or discussing these terms, please email Legal@vivun.com. Further, you agree to honor any request from the Information Security team at Vivun to promptly return or destroy all copies of confidential information and all notes related to the Confidential Information.

In honor of our commitment to collaboration and transparency, Vivun will not withhold approval of disclosure unless Vivun believes, in its sole opinion and at its sole discretion, that confidentiality is required to avoid material harm to Vivun or to any other party, generally.

You must comply with all applicable laws, rules and regulations (including those local to you) with respect to your activities related to Vivun's Vulnerability Disclosure Program. Presently, no awards are available for any respondents/participants of this program. However, if Vivun, in its sole discretion, determines you are eligible for any reward as part of this program, such rewards will not be issued to you if you are (a) in an US embargoed country or (b) on an US Government list of sanctioned or restricted individuals, or affiliated with any sanctioned or restricted entities. Further any reward shall be considered non-transferrable.

Vivun reserves the right to modify the terms and conditions of this Vulnerability Disclosure Program and your participation in the Program constitutes acceptance of all terms. Please check this site regularly as we routinely update our Vulnerability Disclosure Program terms and eligibility, which are effective upon posting. We reserve the right to cancel this Program at any time and without any notice to any participants.

Safe Harbor

Any activities conducted in a manner consistent with this Program on only those assets and activities defined herein as "in-scope" will be considered authorized conduct and we will not initiate legal action against you. Any activities conducted on those assets or activities defined herein as "out-of-scope" shall result in immediate legal action against you and any affiliated parties.