VULNERABILITY DISCLOSURE POLICY

This document outlines Foregenix' Vulnerability Disclosure Policy in relation to vulnerabilities identified by Foregenix during the course of its penetration testing engagements. Foregenix believes in coordinated vulnerability disclosure hence we have gone to great lengths to balance this policy accordingly.

1. Upon identification of a vulnerability in a product, Foregenix will attempt to contact the security contact for the related vendor via email and/or telephone. If no security contact is known or listed for the vendor, Foregenix will attempt to identify one by querying other public vendor contacts. When a security contact is identified Foregenix will send:
    a. A detailed description of the vulnerability
    b. Steps to reproduce it
    c. A disclosure date, normally set in 90 calendar days from the vulnerability disclosure date.
2. If no response is received from the vendor security contact within a week the vulnerability is resent however the disclosure date remains unaltered.
3. If no response is received from the vendor security contact within a week the vulnerability is resent however the disclosure date is reduced to 14 calendar days.
4. If no response is received from the vendor until the disclosure date, the vulnerability is disclosed to the public.
5. Foregenix is willing to extend the disclosure date should extenuating circumstances prevent the vendor from producing a fix within the allocated time or the issue is too complex to address. These will be discussed on a per case basis.
6. If at any time, prior to the agreed disclosure date, details about the vulnerability are made known to the public either by a third party or active exploitation, Foregenix will consider the vulnerability in the public domain and will coordinate any further steps with the affected vendor in a matter of urgency.
7. Vendors are expected to provide updates to Foregenix with regards to the status of the reported vulnerability.
8. Foregenix will contact a CVE Numbering Authority (CNA) and receive a CVE to be used in the disclosure and better tracking of the vulnerability.
9. Vendors are expected to notify Foregenix of the upcoming release of the fix for the identified vulnerability should it fall short of the set disclosure date, in order for Foregenix to publicise the vulnerability (while acknowledging it's resolved status).
10. Vendor should credit Foregenix with the identification of the vulnerability in any publication or notification describing the vulnerability.
11. Foregenix reserves the right to notify its customers with regards to the identified vulnerability prior to the disclosure date
12. Foregenix reserves the right to incorporate defences in its own products and service offerings with regards to the identified vulnerability prior to the disclosure date.
13. Foregenix reserves the right to publish information with regards to the identified vulnerability after its disclosure date on its corporate blog, social media, newsletter, and other publications.