Babblevoice

Penetration Test 2023

Author: Tony Harper | 20/04/2023 | FID0023-1149 | CLIENT CONFIDENTIAL

Fidus

INFORMATION SECURITY

1 Management Summary

Fidus Information Security (Fidus) carried out a penetration test of the environment utilised by Babblevoice. The test took place between Monday 17th April and Tuesday 18th April 2023, with a targeted re-test on 25th May 2023. Testing was carried out by the consultants named in Appendix A of this document. The customer contact was Nicola Hueting (*NHueting@babblevoice.com*).

The overall security posture offered by Babblevoice was found to be of a good standard with no critical or high-risk issues identified during testing. Highlight is drawn to the mitigations in place to prevent cross-site scripting attacks against the application which shows that the customer has taken into account the risk from injection style attacks.

The most significant issue identified concerned excessive open ports being acknowledged by the Fidus consultants that could offer interest to an attacker. Having too many open ports unnecessarily expands the attack surface, providing more entry points for malicious actors to exploit. Each open port represents a potential vulnerability that could be exploited to gain unauthorised access, launch attacks, or infiltrate the Babblevoice network. An example of this was SSH being hosted externally that could allow an attacker to brute force the service with numerous users and password wordlists to gain access to internal resources. Exposing excessive open ports without proper security measures, such as firewalls or intrusion detection systems, can increase the likelihood of successful attacks and compromise the confidentiality, integrity, and availability of Babblevoice's systems and data.

Firewalls rules were exported and provided to the Fidus consultants for review, which only identified a couple of issues that were noted within the report to improve security to the Babblevoice environment. “Any” rules were detected that allow any type of traffic, from any source to any destination, without proper restrictions or filtering. Whilst these rules may provide convenience or ease of configuration, they can result in a lack of granular control and expose Babblevoice's network to potential vulnerabilities.

Fidus offer the recommendation that it would be in the best interest of Babblevoice and service users to remediate all issues highlighted within this report in order to enhance the overall security posture offered. It is suggested that remediation occur in order of vulnerability risk and by the relevant area experts.