Security Vulnerability Disclosure Program

Overview

Realogy is committed to protecting the privacy and security of users of our software tools. Our Vulnerability Disclosure Program is intended to minimize the impact any security flaws have on our tools or their users. Realogy's Vulnerability Disclosure Program covers select software partially or primarily written by Realogy.

Scope: Software Written by Realogy

Realogy's Vulnerability Disclosure Program applies to security vulnerabilities discovered in any of the following software:

https://new.myzap.com
https://bhgre.myzap.com
https://coldwellbanker.myzap.com
https://century21.myzap.com
https://era.myzap.com

In order to qualify, the vulnerability must exist in the latest public release of the software. Only security vulnerabilities will qualify. We would love it if people reported other bugs via the appropriate channels, but since the purpose of this program is to fix security vulnerabilities, only bugs that lead to security vulnerabilities will be eligible. Other bugs will be accepted at our discretion.

Guidelines

Please adhere to the following guidelines when documenting a vulnerability to our disclosure program:

- Do not permanently modify or delete Realogy hosted data.
- Do not intentionally access Realogy data any more than is necessary to demonstrate the vulnerability.
- Do not DDoS or otherwise disrupt, interrupt or degrade our internal or external services.
- Do not share confidential information obtained from Realogy, including but not limited to agent or client information, with any third party.
- Social engineering is out of scope. Do not send phishing emails to, or use other social engineering techniques against, anyone, including Realogy staff, members, vendors, or partners.

In addition, please allow Realogy at least 90 days to fix the vulnerability before publicly discussing or blogging about it. Realogy believes that security researchers have a First Amendment right to report their research and that disclosure is highly beneficial, and understands that it is a highly subjective question of when and how to hold back details to mitigate the risk that vulnerability information will be misused. If you believe that earlier disclosure is necessary, please let us know so that we can begin a conversation.

Reporting

Vulnerability information can give attackers who were not otherwise sophisticated enough to find the problem on their own the very information they need to exploit a security hole in a computer or system and cause harm. Therefore we ask that you privately report the vulnerability to Realogy before public disclosure.

Send an email to information.security@realogy.com, with information about the vulnerability and detailed steps on how to replicate it. Submissions that include detailed information on how to fix the corresponding vulnerability are more likely to be patched more quickly.

We are also happy to accept anonymous vulnerability reports.

We will make every effort to respond to valid reports within seven business days.

The validity of a vulnerability will be judged at the sole discretion of Realogy.

Questions

If you have any questions about our vulnerability disclosure policy, please email information.security@realogy.com