Vulnerability Reporting Policy (August 2022)

Digital Alert Systems (DAS) acknowledges the valuable role of independent security researchers. DAS is expanding our commitment to working with security researchers to verify and address potential vulnerabilities properly reported to us.

This Policy enables users to submit vulnerabilities and exploitation techniques ("**Vulnerabilities**") to DAS about its products and services ("**Products"**). DAS may change this Policy at any time, for any reason. DAS commits to working with researchers to understand and resolve the issue quickly (including an initial confirmation of receipt of a Report within 72 hours of submission). We commit to acknowledging these contributions, such as through citation in our release notes, from the first to report the issue, and we make a code or configuration change based on the subject.

Reporting Process

- Each vulnerability submitted to DAS shall be a **"Report"**. Reports must be sent to security@digitalalertsystems.com. The person/entity sending the report is the **"Submitter"**. In the initial email, the Submitter should specify the vulnerability details and specific product version numbers used to validate the research. DAS asks the Report to please include as much of the following information as possible:
    - Type of issue (buffer overflow, SQL injection, cross-site scripting, etc.)
    - Product and version that contains the bug or URL for an online service
    - Security updates or other updates for the product installed
    - Any special configuration required to reproduce the issue
    - Step-by-step instructions to reproduce the issue
    - Proof-of-concept or exploit code
    - Impact of the issue, including how an attacker could exploit the issue
- The above details of the suspected vulnerability must be sent by email to security@digitalalertsystems.com to ensure any vulnerability report or correspondence is forwarded to the current members of the security team.
- Do not send correspondence to individual email addresses, or group addresses other than security@digitalalertsystems.com.
- DAS is not responsible for Reports that we do not receive for any reason. If no confirmation email is not received after making a Report, notify DAS at security@digitalalertsystems.com to ensure the Report was received.

Report License

DAS is not claiming any ownership rights to the Report. However, by providing any Report to DAS, the Submitter:

- grants DAS the following non-exclusive, irrevocable, perpetual, royalty-free, worldwide, sub-licensable license to the intellectual property in the Report: (i) to use, review, assess, test, and otherwise analyze the Report; (ii) to reproduce, modify, distribute, display and perform publicly, and commercialize and create derivative works of the Report and all its content, in whole or in part; and (iii) to feature the Report and all of its content in connection with the marketing, sale, or promotion of this program or other programs (including internal and external sales meetings, conference presentations, tradeshows, and screenshots of the Report in press releases) in all media (now known or later developed);
- agrees to sign any documentation that may be required for us or our designees to confirm the rights granted above;
- understands and acknowledges that DAS may have developed or commissioned materials similar or identical to the Report, and waiver of any claims having resulted from any similarities to the Report;
- represents and warrants that the Report is unique work, not using information owned by another person or entity, and have the legal right to provide the Report to DAS.

Confidentiality and Restrictions on Disclosure

For the protection of our customers, DAS generally does not disclose, discuss, or confirm security issues until a full investigation is complete and any necessary patches or releases are available. Please do not publicly disclose any details of the Report, the Vulnerability, an indicator of Vulnerability, or the content of information rendered available by a vulnerability until we have responded and have been afforded a reasonable time frame to respond. We endeavor to address each vulnerability report promptly. DAS requires that Reports remain confidential and cannot be disclosed to third parties or as part of paper reviews or conference submissions. After the vulnerability is fixed, you can make available high-level descriptions of your research and non-reversible demonstrations.

We require that detailed proof-of-concept exploit code and details that would make attacks easier on customers be withheld for at least 60 days after the vulnerability is fixed. DAS will notify the Submitter when the vulnerability in the Report is fixed.

Public Recognition

DAS may publicly recognize individuals who have contributed Reports. DAS, at its discretion, may recognize the Submitter on web properties, release notes, or other printed materials unless explicitly asked not to include such attributions.

Code of Conduct

While we encourage reporting any vulnerabilities discovered in a responsible manner, certain types of conduct - including but not limited to the following - are expressly prohibited:

- Performing malicious or unlawful actions against DAS, its employees, or its customers (including but not limited to Harassment, Cyberstalking, Brute Force, Denial of Service, Defamatory or Libelous Statements, Phishing, Vishing);
- Compromising the privacy or safety of any DAS employee or third parties;
- Performing any action that potentially endangers the safety of lives or property;
- Accessing or attempting to access data or information that does not belong to the Submitter;
- Exfiltrating any data that does not belong to the Submitter;
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to the Submitter;
- Conducting any physical or electronic attack on DAS personnel, property, or data centers;
- Social engineering any DAS service desk, employee, or contractor;
- Exploiting any vulnerability beyond the minimal amount of testing required to prove that a vulnerability exists or to identify an indicator related to a vulnerability;
- Conducting vulnerability testing of anything other than test accounts;
- Violating any Federal, state, or local laws, or breaching any agreements.

Safe Harbor

Testing and reporting activities conducted in accordance with this Policy, including its Code of Conduct, are protected by a Safe Harbor, meaning we will not initiate legal action against a Submitter. We consider security research and vulnerability disclosure activities consistent with this policy to be “authorized” conduct under the Computer Fraud and Abuse Act, the DMCA, NY Penal Law 156.05, NY Penal Law 156.10, and other applicable computer use laws. Notwithstanding the foregoing, we may have a legal obligation to report certain activities as related to regulated products and services.

If a third-party initiates legal action against the Submitter in connection with activities conducted under our Policy, we will take steps to make it known that these actions were conducted in compliance with DAS’ Vulnerability Disclosure Policy. If the security research involves the networks, systems, information, applications, products, or services of a third party (which is not us), we cannot bind that third party, and they may pursue legal action or law enforcement notice. We cannot and do not authorize security research in the name of other entities and cannot in any way offer to defend, indemnify, or otherwise protect the Submitter from any third party.

In operating this Policy, DAS does not waive any rights that it may have by not exercising (or delaying the exercise of) such rights. Additionally, if the Submitter violates the Policy, DAS retains all rights and other remedies available to it at law or in equity, including the rights to seek injunctive, specific performance, or other equitable relief.

Thank you for helping us keep DAS' customers and data safe. Please submit a report to us before engaging in conduct that may be inconsistent with our Rules.