Responsible Disclosure Policy

Data security is a top priority for Ortto, and Ortto believes that working with skilled security researchers can identify weaknesses in any technology.

If you believe you've found a security vulnerability in Ortto's service, please notify us; we will work with you to resolve the issue promptly.

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by completing this form. We will respond within five business days.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within ten business days of disclosure, but in some cases may need more time.
- Make a good faith effort to avoid violating privacy, destroying data, interrupting or degrading the Ortto service. Please only interact with accounts you own or for which you have explicit permission from the account holder.
- Bug bounties are on a first-come, first-served basis. If your report is a duplicate, we will inform you of its disclosure timeline and keep you updated on its progress.

Exclusions

While researching, we'd like you to refrain from:

- Denial of Service (DoS/DDoS)
- Spamming
- Social engineering or phishing of Ortto employees, customers, or contractors
- Any physical attacks against Ortto's property, employees, or data centers
- Running automated scans without checking with us first
- Intentionally attacking / compromising our end users or their customers in any way

Specifics

If you need an account to test on, please make a free trial and put bughunt<something unique> in the company name. This will help us internally handle our response in the event of any unintended disruption of service or detection of suspicious activity.

If you manage to get a shell or remote code execution on any of our servers, please create a bug contact file in the home directory of the user that was compromised (if possible). Verify your success then stop and report the vulnerability to us immediately.

Please try to provide a comprehensive report of what you find / how to reproduce the issue.
If you feel uncertain about what is allowed / might cause denial of service please contact us to clarify, prior to proceeding with any action.

We handle each report on a case by case basis, but we do provide bug bounty payments to reports which we think clearly identify and explain serious security issues. Our payouts are in proportion to the severity, clarity, and helpfulness of the report.

Safe Harbor

Activities conducted in a manner consistent with this policy will be considered authorized conduct, and we will not initiate legal action against you. Our services are hosted, used and interact with many cloud providers, and we cannot guarantee they will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Changes

We may revise these guidelines from time to time. To get an updated version of this document please email security@ortto.com, or visit: https://ortto.com/.well-known/security.txt and download the document linked under “Policies”.

Contact

Ortto is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at security@ortto.com.

Employees and Explicitly Hired Security Contractors

If you have an existing penetration testing contract with Ortto then you should refer to the terms of that contract instead of this document.

If you are an employee of Ortto you are ineligible for bug bounties, but you must report any security issues you discover to an appropriate Senior Engineer or Engineering Manager. Failure to do so or violation of this policy may result in disciplinary actions.

Ortto Vulnerability Management & Patch Program

Ortto's Vulnerability Management policies and procedures describe what systems are in place to monitor for new vulnerabilities, how often vulnerabilities are addressed, and the way in which those vulnerabilities are addressed.

On average, 20-30 new vulnerabilities are released into the wild every day. Ortto's internal vulnerability monitoring and external vulnerability scanning are in place to keep up with new threats while validating security controls put in place so that Ortto's security posture is maintained.

Vulnerability Management & Patch Policy

- Ortto performs internal vulnerability scanning and package monitoring on a constant basis using: AWS Inspector, GitHub and Vanta
- The Engineer(s) is responsible for communicating detected vulnerabilities and package updates needed to the appropriate Engineering staff for resolution. Engineering staff responsible for various infrastructure components are responsible for resolving detected vulnerabilities in a timely manner as defined by Ortto's timing standards, as defined below.

Severity & Timing

Ortto defines the severity of an issue via industry recognized Common Vulnerability Scoring System (CVSS) scores, which all modern scanning and continuous monitoring systems utilize. The CVSS provides a way to capture the characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

All vulnerabilities will be addressed within reasonable timelines as defined by company procedural commitments.

We reserve the right to subjectively factor in real world applicability to our score, but generally we strive to be as objective and fair as possible with our scoring.

Low Severity: 0.1 - 3.9

Low severity vulnerabilities are likely to have very little impact on the business, perhaps because they require local system access.

Medium Severity: 4.0 - 6.9
Medium severity vulnerabilities usually require the same local network or user privileges to be exploited.

High Severity: 7.0 - 8.9
High severity vulnerabilities are typically difficult to exploit but could result in escalated privileges, significant data loss, and/or downtime.

Critical Severity: 9.0 - 10.0
Critical severity vulnerabilities likely lead to root level compromise of servers, applications, and other infrastructure components. If a critical vulnerability cannot be addressed within timelines as defined, an incident response ticket will be opened, documenting what interim remediation has been made.

Bounty Rates

Our latest and up-to-date bug bounty rates can be found at https://ortto.com/security/

Responsibility

The CTO is responsible for this policy being followed.

Last updated: 10th November 2022