How to report security issues on SONiC

SONiC project takes the security of our software products and services seriously, which includes all source code repositories managed through our GitHub organizations, which are listed here. We leverage Microsoft Security Response Center (MSRC) to analyze/manage/categorize vulnerability issues found.

If you believe you have found a security vulnerability in any SONiC repository that meets the following definition of a security vulnerability, please report it to us as described below. **Please do not report security vulnerabilities through public GitHub issues.**

Instead, please report them to the Microsoft Security Response Center (MSRC) at https://msrc.microsoft.com/create-report.

If you prefer to submit without logging in, send email to secure@microsoft.com. If possible, encrypt your message with our PGP key; please download it from the Microsoft Security Response Center PGP Key page.

You should receive a response within 24 hours. If for some reason you do not, please follow up via email to ensure we received your original message. Additional information can be found at microsoft.com/msrc.

Please include the requested information listed below (as much as you can provide) to help us better understand the nature and scope of the possible issue:

- Type of issue (e.g. buffer overflow, SQL injection, cross-site scripting, etc.)
- Full paths of source file(s) related to the manifestation of the issue
- The location of the affected source code (tag/branch/commit or direct URL)
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue
- Proof-of-concept or exploit code (if possible)
- Impact of the issue, including how an attacker might exploit the issue

This information will help us triage your report more quickly.

If you are reporting for a bug bounty, more complete reports can contribute to a higher bounty award. Please visit Microsoft Bug Bounty Program page for more details about our active programs.

Preferred Languages

We prefer all communications to be in English.

Policy

SONiC project follows the principle of Coordinated Vulnerability Disclosure.