

Advanced Sterilization Products®

Vulnerability Disclosure Policy for Reporters

Reporters MUST adhere to the following guidelines.

1. GENERAL

- Reporters MUST comply with all applicable laws and regulations in connection with security research activities or other participation in this vulnerability disclosure program.
- Reporters MUST abide by all ASP Terms of Service(s).
- Reporters SHOULD make a good faith effort to notify and work directly with the affected vendor(s) or service providers prior to publicly disclosing vulnerability reports.

2. SCOPE OF AUTHORIZED TESTING

- Reporters MAY ONLY test ASP hardware and software sold to customers with the explicit written permission of that customer ("Authorized Equipment"), to detect a vulnerability for the sole purpose of providing ASP information about that vulnerability. "Authorized Equipment" does not include ASP web sites and properties.
- Reporters SHOULD only test against test accounts owned by the Reporter or with explicit written permission from the account holder if they abide by the Terms of Service for that account.
- Reporters MUST avoid any harm to ASP's information systems, products, and customers.
- Reporters SHOULD contact ASP at productsecurity@asp.com if at any point you are uncertain of whether to proceed with testing.

3. COORDINATION WITH ASP

- Reporters SHOULD submit vulnerability reports, including any ASP websites and properties, to ASP via email at productsecurity@asp.com.
- Reporters SHOULD submit high-quality reports that contain sufficient descriptive details to permit ASP to reproduce the vulnerable behavior accurately.
- Reporters SHOULD NOT report unanalyzed crash dumps or fuzzer output unless accompanied by a sufficiently detailed explanation of how they represent a security vulnerability.
- Reporters MAY include a proof-of-concept exploit if available.
- Reporters MAY request that their contact information be withheld from any affected vendor(s) outside of ASP.
- Reporters MAY request not to be named in the acknowledgments of ASP's public disclosures.

- Reporters **MUST NOT** require ASP to enter a customer relationship, non-disclosure agreement (NDA), or any other contractual or financial obligation as a condition of receiving or coordinating vulnerability reports.
- ASP **SHALL** confirm receipt of the vulnerability report with the Reporter.
- ASP **MAY** investigate the vulnerability report and inform the reporter through the means defined in the report submission.
- ASP **MAY** contact the vulnerability reporter for more information if ASP cannot validate the reported vulnerability.
- ASP **MAY** communicate with the vulnerability reporter on the mitigation status.
- ASP **MAY** communicate with the vulnerability reporter when a mitigation has been validated and when it will be released to ASP customers.
- ASP **MAY** attribute the vulnerability reporter in any security advisories ASP publishes about the vulnerability the reporter discovered. The vulnerability reporter will have the option to opt-out of being attributed, at reporter's discretion.

4. COORDINATION WITH VENDORS

- If the Reporter finds a vulnerability in an ASP hardware or software product due to a vulnerability in a generally available product or service, the Reporter **MAY** report the vulnerability to the affected vendor(s), service provider(s), or third-party vulnerability coordination service(s) to enable the product or service to be fixed.

5. COORDINATION WITH OTHERS

- Reporters **SHOULD NOT** disclose any details of any ASP hardware or software vulnerability or any indicators of vulnerability to any third party.

6. PUBLIC DISCLOSURE

- Reporters **MAY** disclose to the public the prior existence of vulnerabilities already fixed by ASP, including potential details of the vulnerability, indicators of vulnerability, or the nature (but not the specific content) of information rendered available by the vulnerability.
- Reporters choosing to disclose to the public **SHOULD** do so in prior consultation with ASP.
- Reporters **MUST NOT** disclose any incidental proprietary data revealed during testing.

ASP RESERVES THE RIGHT TO DEVIATE FROM THESE GUIDELINES IN SPECIFIC INSTANCES.