

---

## Product security disclosure policy

This policy outlines how the SOFAR handles responsible vulnerability disclosure to product distributor, ODM customers, product vendor, and the general public. SOFAR will responsibly and promptly notify the appropriate product vendor of a security flaw with their product(s) or service(s). The first attempt at contact will be through any appropriate contacts or formal mechanisms listed on the SOFAR Web site, or by sending an e-mail to [info@sofarsolar.com](mailto:info@sofarsolar.com) with the pertinent information about the vulnerability. Simultaneous to the distributor notification, protection filters may be distributed to ODM customers through approved channels.

If a vendor fails to acknowledge SOFAR initial notification within five business days, SOFAR will attempt a second formal attempt to contact a representative for that vendor. If a vendor fails to respond after an additional five business days following the second notification, SOFAR may rely on an intermediary to try to establish contact with the vendor. If SOFAR exhausts all reasonable means in order to contact a vendor, then SOFAR may issue a public advisory disclosing its findings fifteen business days after the initial contact.

If a vendor response is received within the time frame outlined above, SOFAR will allow the vendor 4-months (120 days) to address the vulnerability with a security patch or other corrective measure as appropriate. At the end of the deadline, if a vendor is not responsive or unable to provide a reasonable statement as to why the vulnerability is not fixed, the SOFAR will publish a limited advisory including mitigation in an effort to enable the defensive community to protect the user. We believe that by taking these actions, the vendor will understand the responsibility they have to their customers and will react appropriately. Extensions to the 120-day disclosure timeline are up to the sole discretion of the SOFAR and will only be granted in rare circumstances.

For vulnerability disclosures resulting from an incomplete or otherwise faulty security patch, SOFAR will follow a tiered disclosure timeline. For Critical-rated bugs where active exploitation is detected or imminent, the vendor will have 30 days to produce a new security patch or other corrective measure. For Critical- and High-severity vulnerabilities where the original patch does offer some protection and exploitation is not imminent, vendors will be given a disclosure window of 60 days. All other reports in this category will be given a time of 90 days. For additional details on this portion of our disclosure policy, please refer to this [blog](#).

If a product vendor is unable to, or chooses not to, patch a particular security flaw, SOFAR will offer to work with that vendor to publicly disclose the flaw with some effective workarounds. In no cases will an acquired vulnerability be “kept quiet” because a product vendor does not wish to address it. To maintain transparency into our process, we plan on publishing a summary of the communication we've had with the vendor regarding the issue. We hope that this level of insight into our process will allow the community to better understand some of the difficulties vendors have when remediating high-impact bugs. SOFAR will make every effort to work with vendors to ensure they understand the technical details and severity of a reported security flaw.

SOFAR will formally and publicly release its security advisories on our Web site. Only advisories listed on the website should be considered official SOFAR advisories.