ALERT LOGIC®
Security. Compliance. Cloud.

Alert Logic, Inc. Vulnerability Disclosure policy

The purpose of the Alert Logic, Inc. ("Alert Logic") Vulnerability Disclosure Policy ("Policy") is to track undisclosed vulnerabilities discovered by Alert Logic research and also to educate vendors to Alert Logic of the vulnerability findings applicable to such vendor. Alert Logic intends to provide timely warning to Alert Logic vendors such that they will reasonably have time to supply a patch or a work around prior to the public disclosure of the vulnerability. Alert Logic's goals are to avoid unnecessarily damaging the reputation of the applicable vendor, while at the same time facilitating the education of Alert Logic customers through appropriate disclosure of potential vulnerabilities which may impact such customers. Alert Logic intends to support its vendors as is reasonably practicable to be able to mitigate the applicable vulnerability. Alert Logic seeks better clarity and education for newly discovered vulnerabilities within the security community.

The following details the steps which will be generally used by Alert Logic in applying the Policy:

1. The applicable vendor which is subject to the discovered vulnerability will generally be given 5 days ("Vendor Response Period") from the date of initiation of contact by Alert Logic for a response back, however Alert Logic may shorten this Vendor Response Period if Alert Logic determines that such is in the best interest of Alert Logic or its customers or the public.
2. If no response has been received by Alert Logic within the Vendor Response Period, Alert Logic will assess the risk to Alert Logic, its customers, or the public, of the disclosure or non-disclosure of the vulnerability. Alert Logic may choose to (i) take no immediate action; (ii) expose the vulnerability to one or more of its customers on a confidential or non-confidential basis; or (iii) disclose the vulnerability publicly.
3. Alert Logic intends to use reasonable efforts to support the applicable vendor regarding the disclosed vulnerability and requests for additional information. As practicable, reasonable details will be provided to the applicable vendor on request to assist in replicating the vulnerability.
4. The vendor is responsible for providing Alert Logic with regular status updates regarding its resolution of the vulnerability. If the vendor does not reply to communicatation from Alert Logic at any stage of the resolution process for more than 5 days after the last date of such communication from Alert Logic, Alert Logic will consider vendor to be non- responsive and will take such non-responsiveness into consideration in its analysis of the risks and rewards of public disclosure to potential victims of exploitation of the vulnerability.
5. Alert Logic intends to encourage a joint press release by Alert Logic and the applicable vendor of the Alert Logic vulnerability findings and will encourage the appropriate credit to Alert Logic and its researcher by name.
6. The vendor will be given a maximum of 90 days ("Waiting Period") after date of the initial Alert Logic contact initiation date to release a patch before Alert Logic will disclose the vulnerability publicly.
7. If a third party publicly discloses the vulnerability during the Waiting Period, Alert Logic will consider the vulnerability public and will work as practicable with applicable vendor for immediate disclosure by Alert Logic.
8. If Alert Logic is made aware of or discovers the vulnerability being used in the wild, this fact will be an important factor considered by Alert Logic in determining if public disclosure is appropriate.
9. Full details and deep technical explanation of the exploitation of the vulnerability that is rated as critical may, in the sole discretion of Alert Logic, be withheld for up to 14 days after public disclosure to allow for affected organisations to have an opportunity to remediate.