ZIMPERIUM
MOBILE DEFENSE

# *Zimperium Zero Day Disclosure Policy*

## Summary

The following *Zimperium Zero Day Disclosure Policy* outlines how Zimperium handles responsible vulnerability disclosure to product vendors, Zimperium customers, and the general public. It also reassures product vendors that there is a professional and standard set of guidelines they can expect to be utilized throughout the disclosure process.

## Disclosure Policy

Zimperium 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 vendor Web site, or by sending e-mail to support@company.com with the pertinent information about the vulnerability. Simultaneous with the vendor being notified, Zimperium may distribute new security to its customers' zIPS devices.

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

If a vendor response is received within the timeframe outlined above, Zimperium will allow the vendor six (6) months to address the vulnerability with a patch. 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, Zimperium will publish a limited advisory including mitigation in an effort to enable the defensive community to protect the user. We believe that by doing so the vendor will understand the responsibility they have to their customers and will react appropriately.

We realize some issues may take longer than the deadline due to complexity and compatibility reasons and we are willing to work with vendors on a case-by-case basis. To maintain transparency into our process, if any vulnerability is given an extension we plan on publishing the communication we've had with the vendor regarding the issue once it is patched. 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. Zimperium will make every effort to work with vendors to ensure they understand the technical details and severity of a reported security flaw. If a product vendor is unable to, or chooses not to, patch a particular security flaw, Zimperium 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.

Zimperium will formally and publicly release its security advisories on its Web site and on selected security mailing list outlets.