Security Policy

How SalesTim handles security vulnerabilities

As a provider of products and services for many organizations, we recognize how important it is to help protect user privacy and security.
We understand that secure products are instrumental in maintaining the trust users place in us and we strive to create innovative products that both serve user needs and operate in the user's best interest.

Supported Versions

The following versions of SalesTim are currently being supported with security updates.

Version	Supported
3.x.x	:white_check_mark:
2.2.x	:white_check_mark:
1.x.x	:x:

Reporting a Vulnerability

If you believe you have discovered a vulnerability in a SalesTim product or have a security incident to report, please send us a message to **security@salestim.com** (english as a preferred languages) that includes a detailed reports with reproducible steps.

If you feel the need, please use our **PGP public key** to encrypt your communications with us.

SalesTim's vulnerability disclosure policy

We believe that vulnerability disclosure is a two-way street. Vendors, as well as researchers, must act responsibly.
This is why SalesTim adheres to a 90-day disclosure deadline.
We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix.
That deadline can vary in the following ways: - If a deadline is due to expire on a weekend or US public holiday, the deadline will be moved to the next normal work day. - Before the 90-day deadline has expired, if a vendor lets us know that a patch is scheduled for release on a specific day that will fall within 14 days following the deadline, we will delay the public disclosure until the availability of the patch. - When we observe a previously unknown and unpatched vulnerability in software under active exploitation (a "0day"), we believe that more urgent action—within 7 days—is appropriate. The reason for this special designation is that each day an actively exploited vulnerability remains undisclosed to the public and unpatched, more devices or accounts will be compromised. Seven days is an aggressive timeline and may be too short for some vendors to update their products, but it should be enough time to publish advice about possible mitigations, such as temporarily disabling a service, restricting access, or contacting the vendor for more information. As a result, after 7 days have elapsed without a patch or advisory, we will support researchers making details available so that users can take steps to protect themselves. As always, we reserve the right to bring deadlines forwards or backwards based on extreme circumstances. We remain committed to treating all vendors strictly equally. SalesTim expects to be held to the same standard.

This policy is strongly in line with our desire to improve industry response times to security bugs, but also results in softer landings for bugs marginally over deadline.
Creating pressure towards more reasonably-timed fixes will result in smaller windows of opportunity for blackhats to abuse vulnerabilities.
In our opinion, vulnerability disclosure policies such as ours result in greater overall safety for users of the Internet.