# Security Policy

Full details of the Automattic Security Policy can be found on [automattic.com](https://automattic.com/security/).

## Supported Versions

Generally, only the latest version of Jetpack and its associated plugins have continued support. If a critical vulnerability is found in the current version of a plugin, we may opt to backport any patches to previous versions.

## Reporting a Vulnerability

Our HackerOne program covers the below plugin software, as well as a variety of related projects and infrastructure:

* [Jetpack](https://jetpack.com/)
* Jetpack Backup
* Jetpack Boost
* Jetpack CRM
* Jetpack Protect
* Jetpack Search
* Jetpack Social
* Jetpack VideoPress

**For responsible disclosure of security issues and to be eligible for our bug bounty program, please submit your report via the** [**HackerOne**](https://hackerone.com/automattic) **portal.**

Our most critical targets are:

* Jetpack and the Jetpack composer packages (all within this repo)
* Jetpack.com -- the primary marketing site.
* cloud.jetpack.com -- a management site.
* wordpress.com -- the shared management site for both Jetpack and WordPress.com sites.

For more targets, see the In Scope section on [HackerOne](https://hackerone.com/automattic).

*Please note that the* ***WordPress software is a separate entity*** *from Automattic. Please report vulnerabilities for WordPress through* [*the WordPress Foundation's HackerOne page*](https://hackerone.com/wordpress)*.*

## Guidelines

We're committed to working with security researchers to resolve the vulnerabilities they discover. You can help us by following these guidelines:

* Follow [HackerOne's disclosure guidelines](https://www.hackerone.com/disclosure-guidelines).
* Pen-testing Production:
  + Please **setup a local environment** instead whenever possible. Most of our code is open source (see above).
  + If that's not possible, **limit any data access/modification** to the bare minimum necessary to reproduce a PoC.
  + ***Don't* automate form submissions!** That's very annoying for us, because it adds extra work for the volunteers who manage those systems, and reduces the signal/noise ratio in our communication channels.
  + To be eligible for a bounty, all of these guidelines must be followed.
* Be Patient - Give us a reasonable time to correct the issue before you disclose the vulnerability.

We also expect you to comply with all applicable laws. You're responsible to pay any taxes associated with your bounties.