**Product Security**

Tesla values the work done by security researchers in improving the security of our products and service offerings. We are committed to working with this community to verify, reproduce, and respond to legitimate reported vulnerabilities. We encourage the community to participate in our responsible reporting process. To register as a pre-approved, good-faith security researcher and register a vehicle as a research-registered vehicle, please submit requests to [VulnerabilityReporting@tesla.com](mailto:VulnerabilityReporting@tesla.com).

**For vehicle or energy product**

While we use [Bugcrowd](https://bugcrowd.com/tesla) as a platform for rewarding all issues, please report vehicle and product related issues directly to [VulnerabilityReporting@tesla.com](mailto:VulnerabilityReporting@tesla.com), using our [PGP](https://www.tesla.com/sites/default/files/downloads/teslavulnerabilitypgp.asc) key to encrypt reports containing sensitive information.

**Third-party bugs**

If issues reported to our bug bounty program affect a third-party library, external project, or another vendor, Tesla reserves the right to forward details of the issue to that party without further discussion with the researcher. We will do our best to coordinate and communicate with researchers through this process.

**Responsible Disclosure Guidelines**

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. To encourage responsible reporting, we will not take legal action against you nor ask law enforcement to investigate you provided you comply with the following Responsible Disclosure Guidelines:

* Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC). Any vulnerability that implicates functionality not resident on a research-registered vehicle must be reported within 168 hours and zero minutes (7 days) of identifying the vulnerability.
* Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our services.
* Do not modify or access data that does not belong to you.
* Give Tesla a reasonable time to correct the issue before making any information public.
* Alter only vehicles that you own or have permission to access.
* Do not compromise the safety of the vehicle or expose others to an unsafe condition.
* Security research is limited to the security mechanisms of the Infotainment binaries, Gateway binaries, Tesla-developed ECU’s, and energy products.

For the avoidance of doubt,

* If, through your good-faith security research, you (a pre-approved, good-faith security researcher) cause a software issue that requires your research-registered vehicle to be updated or "reflashed," as an act of goodwill, Tesla shall make reasonable efforts to update or "reflash" Tesla software on the research-registered vehicle by over-the-air update, offering assistance at a service center to restore the vehicle's software using our standard service tools, or other actions we deem appropriate. Tesla has complete discretion as to the software or other assistance that will be provided and it may be only for a limited number of times. Tesla's support does not extend to any out-of-pocket expenses (e.g. towing) incurred by you. Tesla reserves the right to limit the number of service requests per pre-approved, good-faith researcher and unregister a research-registered vehicle at any time.
* Tesla considers that a pre-approved, good-faith security researcher who complies with this policy to access a computer on a research-registered vehicle or energy product has not accessed a computer without authorization or exceeded authorized access under the Computer Fraud and Abuse Act ("CFAA").
* Tesla will not bring a copyright infringement claim under the Digital Millennium Copyright Act ("DMCA") against a pre-approved, good-faith security researcher who circumvents security mechanism, so long as the researcher does not access any other code or binaries.
* Tesla will not consider software changes, as a result of good-faith security research performed by a good-faith security researcher, to a security-registered vehicle to void the vehicle warranty of the security-registered vehicle, notwithstanding that any damage to the car resulting from any software modifications will not be covered by Tesla under the vehicle warranty.

**Tesla Security Researcher Hall of Fame**

Tesla appreciates and wants to recognize the contributions of security researchers. If you are the first researcher to report a confirmed vulnerability, we will list your name in our Hall of Fame (unless you would prefer to remain anonymous). You may also be considered for an award if you are the first researcher to report one of the top 3 confirmed vulnerabilities in a calendar quarter. You must comply with our Responsible Disclosure Guidelines (above) to be considered for our Hall of Fame and top 3 awards.

|  |  |  |
| --- | --- | --- |
| **2018** | [UnicornTeam](https://unicorn.360.com) | [Jun Li (@bravo\_fighter)](https://mobile.twitter.com/bravo_fighter), [Qing Yang (@Ir0nSmith)](https://mobile.twitter.com/Ir0nSmith), Yingtao Zeng, Chaoran Wang |
| **2017** | [Keen Security Lab](http://keenlab.tencent.com/) | [Tencent](http://keenlab.tencent.com/) for CVE-2017-9983 and CVE-2017-6261 |
| **2016** | [Keen Security Lab](http://keenlab.tencent.com/) | [Tencent](http://keenlab.tencent.com/) |
|  | [Skygo Team](http://skygo.360.cn/), [USSlab](http://usslab.org/) | [Qihoo360](http://skygo.360.cn/), [Zhejiang University](http://usslab.org/) |
| **2014** | [Eusebiu Blindu](https://twitter.com/testalways) | [@testalways](https://twitter.com/testalways) |
|  | [Muhammed Gazzaly](https://twitter.com/gazly) | [@gazly](https://twitter.com/gazly) |
|  | Jianhao Liu | Qihoo 360 Adlab |
|  | Jiaheng Wang | Zhejiang University |
|  | Yanjing Wu | Zhejiang University |
|  | Wenyuan Xu | Zhejiang University |
|  | [Nitesh Bhatter](https://twitter.com/nbhatter) | [@nbhatter](https://twitter.com/nbhatter) |
| **2013** | Jaime Manteiga |  |
|  | [Anshuman Bhartiya](https://twitter.com/anshuman_bh) | [@anshuman\_bh](https://twitter.com/anshuman_bh) |
|  | [Nitin Goplani](https://twitter.com/nitingoplani88) | [@nitingoplani88](https://twitter.com/nitingoplani88) |
|  | [Issam Rabhi](https://twitter.com/yappare) | [@yappare](https://twitter.com/yappare) |
|  | Ahmad Ashraff |  |
|  | [Phil Purviance](https://twitter.com/superevr) | [@superevr](https://twitter.com/superevr) |
|  | Michael |  |
|  | [Jon](https://twitter.com/bitquark) | [Bitquark Security Research](https://twitter.com/bitquark) |
|  | Jack "fin1te" W |  |
|  | Ch. Muhammad Osama |  |
|  | [Arsiadi Sriyanto](https://twitter.com/donrookie) | [@donrookie](https://twitter.com/donrookie) |
|  | [Nikhil Kumar Srivastava](https://twitter.com/niksthehacker) | [@niksthehacker](https://twitter.com/niksthehacker) |
|  | [Muhammad Shahmeer Maads Security](https://twitter.com/Shahmeer_Amir) | [@Shahmeer\_Amir](https://twitter.com/Shahmeer_Amir) |
|  | [Olivier Beg](https://twitter.com/smiegles) | [@smiegles](https://twitter.com/smiegles) |
|  | [Ashar Javed](https://twitter.com/soaj1664ashar) | [@soaj1664ashar](https://twitter.com/soaj1664ashar) |
|  | [Jay Turla](https://www.tesla.com/about/security) | [HP Fortify](https://www.tesla.com/about/security) |
|  | Haris Mamoun |  |
|  | [Mehmet Ince](https://twitter.com/mmetince) | [@mmetince](https://twitter.com/mmetince) |