How to Submit a Responsible Disclosure

- Parallels Desktop for Mac Pro Edition
- Parallels Desktop for Mac App Store Edition
- Parallels Desktop for Mac Business Edition
- Parallels Desktop for Mac Standard Edition
- Parallels Remote Application Server
- Parallels Toolbox Business Edition
- My Account
- Parallels Toolbox
- Parallels Secure Workspace
- Parallels DaaS
- Parallels Browser Isolation

Parallels is committed to maintaining the security of our systems, products and customer's information. We investigate all legitimate submissions in a timely manner and fix issues based on criticality factors and our release cycle once verified.

Responsible Disclosure Program Submission Policy

Submissions shall meet the following requirements:

- Product vulnerabilities must lead to individual or collective confidentiality, integrity and availability compromise and/or disruption.
- Submission must demonstrate vulnerability was discovered without the use of blackhat techniques and/or violations of our Terms of Service, Terms of Use, End User License Agreement and regulatory obligations.
- Submissions must contain: (1) Product Name, (2) Product Version (3) License or Proof of Purchase (4) hosting OS.
- Submissions must contain Proof of Concept (PoC) demonstrating successful exploitation when mitigations are in place preventing exploitation such as antivirus or IDS/IPS.
- Submitters must have the ability to verify your legal identity along with no known disinterested associations.

Non-valid Submissions

Certain submissions are not valid for Parallels' Responsible Disclosure program:

1. Submissions using PGP or password protected.
2. Requests for payments inclusive of PayPal/Cryptocurrency or other non-traceable monetary exchange systems.
3. Anonymous e-mail addresses that cannot be verified.
4. Submissions related to Application/service owned, managed or hosted by a third-party.
5. Submissions where CVSS scoring is incomplete, thereby rendering the overall score inaccurate

6. Submissions resulting from unsolicited scanning of our infrastructure.
7. Submissions resulting unsolicited scans of our products.
8. A submission combining more than one vulnerability.
9. Submissions related to: Clickjacking, Tab nabbing, Weak Ciphers, UI Redressing, Hyperlink Injection, and Certificate Authority.
10. Submissions from sanctioned counties, nor a person on, or working on behalf of a party identified on any disinterested list maintained by the United States, Canada, Ireland, German, Malta or Swiss governments.
11. Submitters providing covered information such as: credit card or bank account numbers.

This policy is in line with our desire to improve overall Internet safety. Parallels does not waive any rights or claims with respect to activities that are in violation of the law or could be interpreted as such.

Submissions meeting the above requirements may be sent to: security@parallels.com. If your submission meets all requirements and is valid, we will follow-up with you, otherwise ***consider the matter closed*** with **no further communication.**

Parallels thanks security researchers who facilitate new long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities.
