Product Security

Updated: 14 October 2022

At HTC, we recognize how important it is to protect your privacy and security. We understand that secure products are essential in maintaining the trust you place in us to provide products and services to you.

These HTC products are increasingly a combination of innovations from HTC as well as many technology partners. Securing the overall system is thus a joint effort involving HTC, our partners and external security experts.

We believe in and follow a philosophy of Responsible Disclosure which places the end-consumer's interests first. Responsible Disclosure involves privately notifying our partners and vendors of any security vulnerabilities, allowing them to diligently close the vulnerabilities before making full disclosure. While the vulnerability is being closed, we will advise end-consumers of a potential risk only in a way which does not increase the overall risk to end-consumers.

In the case of security vulnerabilities identified in our products, we encourage the reporting party to also place the end-consumers' interests first and apply the philosophy of Responsible Disclosure.

If you have identified any security vulnerability in an HTC product or service or have a security incident to report, please email: security@htc.com . Please include a detailed summary of the issue, the name of the product or service and the POC (Proof of Concept). Also, please make sure that you include correct contact information, such as an email address, by which we can reach you in case we need more information.

We believe that it is good for the overall security of our end-consumers by privately notifying partners or vendors about vulnerabilities in their products and setting reasonable disclosure deadlines in accordance with the severity of the bugs and issues.

We take security issues seriously and will respond promptly to fix verified security issues. Nonetheless, it may take some time to update certain products of ours due to their complexity. Upon receipt of proper notice of legitimate issues, we'll do our best to acknowledge your emailed report, assign resources to investigate the issue and resolve potential problems as quickly as possible.

In addition, upon request of the security professional who has reported a verified security issue, we will do our best to provide updates on our progress addressing the issue to give confidence that we are responsibly addressing the vulnerability.

The combined contributions of all security professionals in the community are essential to keep the community secure. We thank everyone in the community for their continued and joint efforts.

The security@htc.com email address is intended ONLY for the purpose of reporting product or service vulnerabilities. It is NOT for the purpose of requesting technical support to our products or services in the case of, for example, device lost, device hacked or account deletion. All content submitted other than that made specific to security vulnerabilities in our products or services might be dropped from the system. For technical and customer support inquiries, please visit HTC Support .

HTC does not have a public bug bounty program, nor do we provide monetary rewards for publicly reported findings.

HTC will attempt to acknowledge receipt of all submitted reports within seven days.

PGP key information

Due to the sensitive nature of security information, HTC provides a method for you to encrypt emailed report to send to HTC via security@htc.com . You can use HTC's Product Security PGP key to encrypt sensitive information sent via email.

For Product Security latest update, please visit https://www.htc.com/tw/terms/product-security/.

Effective Date: 20 July 2011