

# Responsible Disclosure Procedure

At the Eurocom, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

## **Please do the following:**

- E-mail your findings to [security@eurocom-group.eu](mailto:security@eurocom-group.eu). Optionally encrypt your findings using our PGP Key to prevent this critical information from falling into the wrong hands;
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
- Do not reveal the problem to others until it has been resolved and permission for disclosure is granted;
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

## **What we promise:**

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date;
- If you have followed the instructions above, we will not take any legal action against you in regard to the report;
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission;
- We will keep you informed of the progress towards resolving the problem;
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise); and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

## Our PGP Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
Comment: User-ID: Eurocom Security <security@eurocom-group.eu>  
Comment: Valid from: 12/02/2024 16:44  
Comment: Valid until: 12/02/2027 12:00  
Comment: Type: 255-bit EdDSA (secret key available)  
Comment: Usage: Signing, Encryption, Certifying User-IDs  
Comment: Fingerprint: B8507058D030C6617C40365352EEE45347C9EAE1  
  
mDMEZco8+BYJKwYBBAHaRw8BAQdAixf06HhkozU6lT8Vkc2TUzEqgjoLytaRv54c  
zJzLcCC0LEV1cm9jb20gU2VjdXJpdHkgPHNlY3VyaXR5QGV1cm9jb20tZ3JvdXAu  
ZXU+iJkEEYKAEEWIS4UHBYY0DDGYXxAN1NS7uRTR8nq4QUCZco8+AIbAwUJBaSp  
OAULCQgHAgIiAgYVCgkICwIEFgIDAQIEBwIXgAAKCRBS7uRTR8nq4RMBAP47spzK  
ZorNM/0X9CHxd7DcUUqYoj4xn3RyOE2AZy9eTAD/d1m9CwzoIoJew0wC30Hx5lk8  
8QQazeAe8kumaazhgw640ARlyjz4EgorBgEEAZdVAQUBAQdA7oT+a4ZRZgNwYKM6  
wCGSvaM+tywrdY8Q9SXqf5bNHWQDAQgHiH4EGBYKACYWIS4UHBYY0DDGYXxAN1NS  
7uRTR8nq4QUCZco8+AIbDAUJBaSpOAAKCRBS7uRTR8nq4dLuAQC6j+Pn5xnelbf6  
K7r3ndiiqUDneanbbccue9+vei/frAEAxJU4bdk05+uu/ueRB2bykDC/iylvMvEy  
frjIK7Wb+w4=  
=etAR  
-----END PGP PUBLIC KEY BLOCK-----
```