Are you a customer?

This document and the procedures outlined herein are not intended for general support questions. Please ask those questions in the appropriate channels. Any communication that is not a security disclosure will not be answered.

Please do the following:

- Send your findings to security@eventree.nl *(do not use this for general support inquiries: they will not be answered).*
- 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 solved.
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties.
- 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 5 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 not pass 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)*.

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.

Out of scope:

1. Public API keys found in HTML source code of our website (like public reCAPTCHA tokens).

This is a non-exhaustive list. Please do not report anything in this list, as it is out of scope.

Non-qualifying reports:

Some reports do not qualify because they have a low security impact. Please do not report these issues unless it is demonstrable that it may produce a chained attack with a higher impact.

- HTTP non-200 codes/pages.
- Disclosure of known public files or directories (e.g. robots.txt, /wp-admin).
- Clickjacking and issues only exploitable through clickjacking.
- CSRF on forms that are available to anonymous users (e.g. contact forms).

- Presence of autocomplete or save password functionality.
- Lack of Secure and HTTPOnly cookie flags.
- OPTIONS / TRACE HTTP method use.
- TLS attacks such as BEAST, BREACH and Renegotiation attack.
- TLS Forward Secrecy misconfiguration.
- TLS Insecure Cipher suites.
- Missing DNSSEC.
- Missing HTTP security headers (e.g.: Content-Security Policy).

In scope systems:

- *.eventree.nl
- *.paytree.nl
- *.paytree-network.nl
- *.eventree-network.nl
- *.evntr.nl
- *.ticketsms.nl
- *.festsms.nl
- *.dogsms.nl
- *.paytr.nl
- *.ev-sms.nl
- *.eventree-mailing.nl

This is a non-exhaustive list. If you find anything related to our system that is not included in this list, please feel free to report it.

Encrypting your findings

We have confidence that regular e-mail encryption will be sufficient to ensure the confidentiality of your findings. We offer the opportunity to encrypt your findings using our PGP public key.

PGP Public key: https://assets.eventree.nl/static/eventree-paytree-security-disclosure-public-key.pgp

Or copy it here:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGU4/kQBEAC/ItK4GDBMxH29XJMEZMMxKg5Dx97YmQoJJ0rjPgA13Zywlw/j
9MuAn5zj1xDrvbfcSg8tocBF0iYiPHG5pmCJiy+xKcPt8JjWjnkyq69Ipai0WO2A
6oRJLPdajwtcMNI91jWUfmTd6MZLcLwZoqHw2OPyOvGg6+/+IazdK6cGHw+S1Flw
iY/wFU8F6JUtzeKCJc23KlsXX3fDPGdEXkZxHcbWKsNrgXPsnjeF9QfwNj5B16hK
xsDpv+1c2bQGhAUgxNmT9AgUyP+ar23Z3SfiotM1bpyoQtYIiVpEUpHCyI+9JtVv
u9DRvYLUUNSqa77EBgdcy+DJerGVeBUMtTfseys4XoHkJCduXyxjLdyfJmPZj6pX
OaYIYdnbFvkJMpI5wrNuBhBeADzNmHeryNlIOPub2L1DpjUJUJgZOnIutw87LKW2
EnOD2nd86OtNxY7xkkStdq0DS2GDVYnK27ttCrGn2oCert4t6q9djKtWAl+VKnVd
l3Zo9lJpqJbgZqQJsJ27Fqp3eHhCOwEZoqMRSOAHXLyU16nMcBBIRgVTJbYgqasg
T1cSZdcF3dGL7ON5J7IgHX17/lZ1SJTAlDtB18v7kMp1QwmKlVIcxwPWglNLspOG
I7F3MwH3kPU4MXYgu76+MlH4zLJwv9ivCXx+rfsx+cNx7q6XfZvqD2v16wARAQAB
tFRFdmVudHJlZSBQYXl0cmVlIChFbmNyeXB0IHNlY3VyaXR5IGRpc2Nsb3N1cmVz
IHdpdGggdGhpcyBrZXkpIDxzZWN1cml0eUBldmVudHJlZS5ubD6JAk4EEwEKADgW
IQSGY3cNZP6OYWcjWgrQ+zLp33cilQUCZTj+RAIbAwULCQgHAgYVCgkICwIEFgID
AQIeAQIXgAAKCRDQ+zLp33cilUtJD/405mLA7GJUKORsQAV8sgDWPp8u6LgyK6L7
DgT+VadqEN6OXD9Kaj1b7c7MLaP6lYnidu3SAtLN4IaRQRU21yfpzbEUXSAYeOrd
gzCTfu8PL5yJPhHJJBgLi/haYLEEBWj23qvFLbPMGytjsLlHVpvQI+Ufp0Vssb6g
V2CFxvpd4qiHvonjfavNuj2ieofzg8/u/vvl8nRhD7Z+8WEod/9pIBcft1S+70sT
yPvFScHbWxCfzP4ioM6cofz/uesHkej1fLlKoHodZlqOsi5z3vrcKCYB0WBjBkV2
/0sJqPm9o4rlNRf5Re6J+zSqOH7aN1Ul7SyurGKmpsJzWODkw/P1JcZPLrDmpfox
1vRTxiUaybbwJFPvCN6q2MBKakyT+N6SJqjei9i4GJkDnGnFJLDM+h/2ucOkrePk
tyUsCUf5eyLDFIawkvHedHAKxcAor46J5ecjE2fTBJEpk/bTFU2/emoRgx0aKVUh
ffEJJR9G65nooqA4J9nHBI8RKSTrcpFomQgh2f4g4L4ZR9q5UScAvO8vNk5qc8u6
G7emaN34BZzEmj1SwNfZ+p0+2YqFn0cyLEzywIHWyqtw5nlNwzcQSNIbz8ta6Pzx
hN35bNvgmvHDvOEiPRmbGswmgHPjb8ZaJH11HuTEkyJkekAXN2O8HGPuWhLwODHg
8zX7oqrXe7kCDQRlOP5EARAA6TQ0UmnEMg8asz+ehD+scL6kjcFagLPhmDgVp/Eh
U1mtVc4pOPUWUWImbEm6lqVDZcgDB24oVYOHapeupXZDe6VieUiZ0Xz+YDFzWVSr
9mBQm5Q1MsyxdLCBNSiKFlTIQ/PN7cNWbt9uvxZjJ90hlhMa9VelTgkPIf71ojGb
Vc0yITb/ZwLN+C+CVR6u1M5YfdJi4Bhd/B9jPBrqr2LNaAnkzpUpBaJQA/GrQPch
aTwlWuCCuzbaqatSnKXegbRq8hprSA+6zpgwydJ9YMFITVxcndI7v8n+XQerJgtZ
4UEJrlToriXZ1Nbqe6eK3uk3f3RSVC6hEWqKF56VF+6BTrwBBniYHUHqa9i0akgg
yDhGDGmYTNdh0Ki0LtWHKHpL/2Y0ycVxL5fDQVkrH6erlSGQEp0QRc9qdYeTRGa1
kkMYTNhf66WDyfrgMAHydaB2ntrkQF/rGot0FXz6603duKxPupnDiJNEsGnMveaz
i1foxa0iconV3DFuNKrcVibM75giBt1HPs1DxEuFHhZaICp60IR6nL/Tl98abqpL
myFKJh62ctavMRtmGmFo3ZrrAQzYFFLqBk8IiVINrKdOoSNt+PJrj6NhtHTEa/Un
IHYHgVIZXI6XRrNdZ1ewU7UtZFumkjp4/Uj+o165dxJNEgMgWAIsL29045LYOeak
5cMAEQEAAYkCNgQYAQoAIBYhBIZjdw1k/o5hZyNaCtD7MunfdyKVBQJlOP5EAhsM
AAoJEND7MunfdyKVPIwP/RWsRBm1sz5UtmW6vZfI9BPlFd4f6pZDIfWQLI5N/xpI
kCR7kWKbI310X1ZPRDLqPtqxnLH5rSHNhOGeZr+1iBkGEjCvgbwVwN/EEbPhV2LX
p0vaoOdAP1LuySf3iUQ3Vm1WQRVf3hXn9PlkLu8lwz2X0rTs6P10iturtB+wDtJL
m1cdmwbmPikiA4nH+GxPaHyG3TGd0+jLKHVkt62dkNA5SvgZUNklC1ZnaN2WN9w1
i1i/uMTgaNMEauSqx2wqI25bepYRk7WvsQCleCLneQtyF6bqXQr9AOf/zxT6wwW+
IMVDLHZswZJFikAV6pDSaE1OBlIAlHYoOxV1VSZF1pdYtFILxbLyceHqALu4PAJZ
yPczgCjB1Q2AmvrOZtsE8LTqm0wToqLc80HyU5V6LTIVwq+xAaXHuUOKv9H+Whf3
OfdY96l4tszNKlms/ADBBTJb/Ey+fDDsArDiLYAb/luXJwnreOqm5wUsVX4if/d0
rc06nvDntxDLPdA7JRz0LhWzO1Mw86OA0dpvTMIG4ixpORUxu91n1v4SuQWuYl+p
B2TrkckRaYhrR/lzeTCz0Ulb6nnIeQuII69o/RQ7Iy3IgRNqGT6nbndmqDgkHyRJ
55/mm8RnzS3c4c/w1pQZWKHfsOB0EB9ggLyPjfxwyX52ac7nEIMYpYLtrz0g/+3D
=P1dt
-----END PGP PUBLIC KEY BLOCK-----
```