Aesys Vulnerability Disclosure Policy

Last updated on July 31st 2023

As Aesys we know that any system and infrastructure can be(come) vulnerable. We encourage everyone to report security vulnerabilities. This protects us, our customers, partners and stakeholders and makes the world a little more secure.

1 Safe harbour

We will not take any legal action against activities complying with this policy. If legal actions are initiated by third parties due to activities compliant with this policy, we will take actions to make it known to responsibles and/or legal authorities.

2 Our promise

We will review and respond to your report promptly and conduct an open dialog with you. We will provide a timeline for when we expect the vulnerability to be fixed. We will give you credits for your findings, if desired.

3 Your promise

You promise to use discovered vulnerabilities for no other purpose than reporting them to us. Vulnerabilities are reported exclusively and privately, promptly after detection. You promise to not take actions with the intention to harm us, our customers, partners, or any other stakeholder.

4 Scope

The following activities are explicitly prohibited by our policy:

- Denial of service (including resource-exhaustion, automated scanners with high loads, deleting data, fuzzing, …);
- Spamming;
- Social engineering (including phishing);
- Physical access (including entering or surveilling properties);
- Attacking third-party systems possibly connected to our devices (internal networks, private IPs, workstations, …);
- Installing persistent backdoors.

5 Contact

For reporting any findings, please contact us at security-issue@aesys.com. If you need to communicate us sensible data (e.g. emerged from exploitation of the vulnerability you’ve found) we invite you to send them securely, by encrypting them using our public OpenPGP key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mDMEZMeHuhYJKwYBBAHaRw8BAQdAdRpBy4V9aByPo2hsy7Rv7u2x/4zeeSC4/W38
zvaUWbm0OEFlc3lzIFNlY3VyaXR5IElzc3VlIEhhbmRsaW5nIDxzZWN1cml0eS1p
c3N1ZUBhZXN5cy5jb20+iJMEExYKADsWIQQzs+kwuU4L3ulb1vzOojxj4U8FFwUC
ZMeHugIbAwULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRDOojxj4U8FF6NS
AQCHBY4b3PGOJpooIO3J0PVOhMhBi0ROWTJcmzPoCHZcrwD/bzCBgRtkQLlorbD3
MGJBvHrY7KgE56Xq0u/Bw+vDoAW4OARkx4e6EgorBgEEAZdVAQUBAQdA43wBCLYB
CUBm6V88ZlWwTVHtry7r9RpaeRhShDXeTgEDAQgHiHgEGBYKACAWIQQzs+kwuU4L
3ulb1vzOojxj4U8FFwUCZMeHugIbDAAKCRDOojxj4U8FF7TjAP0VVscJpGZBrsQs
IhvaHqStPulhJ6U+AfETm5zYkHowIwD+Jy0PYwjmhe1ezgZGspfGsYxK3XtRuZUK
0ulwl+hi5gA=
=Z7T1
-----END PGP PUBLIC KEY BLOCK-----
```

Our public PGP key is also available at https://www.aesys.com/aesysadmin/uploads/file/vdp-pgp-key.txt.

6 Thank You

Thanks to all who report security vulnerabilities to us.