Politica di divulgazione delle vulnerabilità

Ultimo aggiornamento: 31 luglio 2023

Politica di divulgazione delle vulnerabilità

Come Aesys siamo consapevoli che qualunque sistema o infrastruttura possa essere (o divenire) vulnerabile. Per questo motivo incoraggiamo chiunque a riportarci eventuali vulnerabilità di sicurezza rilevate nell'utilizzo dei nostri prodotti. Ciò protegge Aesys, i nostri clienti, i nostri partner e contribuisce a rendere il nostro mondo un luogo più sicuro.

1 Difesa dei nostri collaboratori

Non intraprenderemo nessuna azione legale con riferimento ad attività svolte da chiunque in conformità alla politica descritta in questo documento. Nel caso venissimo a conoscenza di azioni legali intraprese da terze parti con riferimento a tali attività, intraprenderemo le azioni necessarie per rendere presente la nostra posizione ai responsabili e/o alle autorità giuridiche competenti.

2 La nostra promessa

Promettiamo di analizzare prontamente le segnalazioni relative alla scoperta di vulnerabilità nei nostri prodotti e di condurre un dialogo aperto con chiunque ci abbia inviato la segnalazione. Promettiamo di definire e condividere con l'interessato cronoprogramma di intervento con chiara indicazione dell'istante entro il quale ci aspettiamo di mitigare la vulnerabilità segnalata. Ci impegniamo a ringraziare pubblicamente le persone e/o gli enti coinvolti nella segnalazione, se questa è la loro volontà.

3 La vostra promessa

Chiunque dovesse scoprire vulnerabilità di sicurezza nei nostri prodotti si impegna a non utilizzare ciò che ha scoperto per finalità diverse dalla segnalazione nei nostri confronti. Le vulnerabilità devono essere segnalate in modo esclusivo ad Aesys, comunicando con noi in modo sicuro, immediatamente dopo esserne venuti a conoscenza.
Chiunque collabori con noi per la segnalazione delle vulnerabilità di sicurezza nei nostri prodotti si impegna a non intraprendere azioni che possano intenzionalmente causare danni ad Aesys e/o ai nostri clienti e partner.

4 Ambito di applicazione

Le seguenti attività sono esplicitamente proibite dalla nostra politica di gestione delle vulnerabilità:

- Denial of service (ivi incluse gli attacchi per esaurimento di risorse, scan ad alto carico, cancellazioni di dati, fuzzing, …);
- Spamming;
- Ingegneria sociale (ivi incluse le pratiche di phishing);
- Accesso fisico (ivi incluse l'ingresso o la sorveglianza di proprietà private);
- Attacco a sistemi di terza parti eventualmente connessi ai nostri prodotti (reti private, workstations, …);
- Installazione di backdoor persistite.

5 Contatti

Per riportare eventuali vulnerabilità di sicurezza, vi invitiamo a contattarci all'indirizzo e-mail security-issue@aesys.com. Se è allegare alla comunicazione dati sensibili, vi inviamo a inviarci la segnalazione in modo sicuro, cifrandola con la nostra chiave pubblica OpenPGP, qui di seguito indicata:

```
-----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-----
```

La chiave pubblica è disponibile anche all'indirizzo web https://www.aesys.com/aesysadmin/uploads/file/vdp-pgp-key.txt.

6 Grazie

Ringraziamo sin d'ora chiunque voglia collaborare con noi riportando eventuali vulnerabilità di sicurezza rilevate durante l'utilizzo dei nostri prodotti.