

Politik for sikkerhed og offentliggørelse af sårbarheder

UnderStack er fabrikant af UnderStack Code i henhold til EU's forordning om cyberrobusthed (CRA). Vi byder rapporter om sårbarheder velkommen og håndterer dem efter princippet om koordineret offentliggørelse.

Sådan rapporterer du

Send en e-mail til security@understack.dk med:

- programversionen (Settings > About & legal) og macOS-versionen;
- en beskrivelse, trin til at genskabe problemet og den virkning, du har observeret;
- om du ønsker at blive krediteret, og i så fald under hvilket navn.

Medtag venligst ikke personoplysninger, der ikke er nødvendige. Maskinlæsbar kontakt: <https://understack.dk/.well-known/security.txt>

Det lover vi

- Kvittering for modtagelse inden for 3 arbejdsdage og en vurdering inden for 10 arbejdsdage.
- Opdateringer mindst hver 14. dag, indtil problemet er løst.
- Mål for rettelser: kritisk 7 dage, høj 30 dage, middel 90 dage, lav i den næste ordinære udgivelse.
- Sikkerhedsopdateringer er gratis og leveres til alle understøttede versioner mindst indtil 31. december 2031.
- En offentlig sikkerhedsmeddelelse, når rettelsen er tilgængelig, hvor du krediteres, hvis du ønsker det.
- Hvis en sårbarhed aktivt udnyttes, indberetter vi den til den kompetente CSIRT og ENISA som krævet i CRA og informerer brugerne om de afhjælpende foranstaltninger, der skal anvendes.

Safe harbour

Forskning i god tro, der følger denne politik, er velkommen, og vi vil ikke tage retslige skridt mod den. Vi beder dig om at: teste kun på systemer og data, du ejer; ikke tilgå, ændre eller opbevare andres data ud over et minimalt proof of concept; ikke forringe tjenester; ikke anvende social engineering eller fysiske angreb; give os rimelig tid (op til 90 dage) til at rette fejlen før offentliggørelse.

Uden for anvendelsesområdet

Kvaliteten af AI-modellers output (forkerte svar er ikke sårbarheder, medmindre de omgår godkendelsessystemet), problemer, der forudsætter en allerede kompromitteret macOS-konto, og sårbarheder i tredjeparters tjenester eller modeller — rapportér disse til deres vedligeholdere, og fortæl os det, hvis den måde, UnderStack Code bruger dem på, forværrer virkningen.

Softwarestyklister (SBOM)

Hver udgivelse indeholder en CycloneDX-SBOM og meddelelser om tredjepartslicenser, som kan ses i Settings > About & legal.