OLVG Coördinated Vulnerability Disclosure beleid

Responsible Disclosure

OLVG hecht veel belang aan de veiligheid van haar (medische) apparatuur, programmatuur en diensten. Ondanks de zorg voor de beveiliging hiervan kan het voorkomen dat er toch sprake is van een kwetsbaarheid. Als u zo'n kwetsbaarheid ontdekt, kunt u dit veilig aan ons melden. Deze aanpak is de zogenaamde Coordinated Vulnerability Disclosure. Op deze manier kan OLVG beschermende maatregelen treffen. ***English version below**

Melding maken van een kwetsbaarheid

Als u een kwetsbaarheid heeft gevonden horen wij dit graag, zodat we zo snel als mogelijk maatregelen kunnen treffen. OLVG wil graag met u samenwerken om onze klanten en systemen nog beter te kunnen beschermen.

Wanneer u via ons Coördinated Vulnerability Disclosure beleid kwetsbaarheden aan ons meldt, dan hebben wij geen reden om juridische consequenties te verbinden aan uw melding, indien u zich houdt aan de volgende regels:

- Verzeker u ervan dat uw melding 'in scope' is. Op www.z-cert.nl/cvd-melden kunt u controleren wat als niet 'in scope' wordt beschouwd.
- U meldt uw bevindingen bij Stichting Z-CERT. Gebruik hiervoor het mailtemplate dat u kunt vinden op **https://www.z-cert.nl/cvd-melden**. Stuur dit volledig ingevuld naar cvd@z-cert.nl, eventueel gebruik makend van Z-CERT's publieke PGP-sleutel. Stichting Z-CERT handelt voor OLVG Coördinated Vulnerability Disclosure meldingen af. Zij werken samen met u als melder en met OLVG om te zorgen dat uw melding wordt opgepakt.
- In uw melding geeft u voldoende informatie, zodat het probleem te reproduceren is. Op die manier kunnen wij het zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden is soms meer informatie gewenst/noodzakelijk. U kunt een proof of concept als bijlage meesturen.
- U misbruikt de geconstateerde kwetsbaarheid niet door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door gegevens van derden in te zien, te verwijderen of aan te passen.
- Als u vermoedt dat u via een kwetsbaarheid medische gegevens kan inzien, vragen wij u dit niet zelf te verifiëren, maar dit door ons te laten doen.
- U deelt uw bevindingen niet met anderen, voordat het is opgelost. Daarnaast vragen wij u om alle vertrouwelijke gegevens die u heeft verkregen, na het dichten van het lek, direct te wissen.
- U doet geen aanval(len) op onze (fysieke) beveiliging d.m.v. social engineering, distributed denial of service, spam, brute-force aanvallen, applicaties van derden en/of andere typen aanvallen.

Hoe wij omgaan met uw melding

- OLVG en Z-CERT behandelen uw melding vertrouwelijk en delen uw persoonlijke gegevens niet met derden zonder uw toestemming, tenzij dit wettelijk verplicht is.
- U krijgt een ontvangstbevestiging van Z-CERT en binnen vijf werkdagen ontvangt u een reactie op uw melding met een beoordeling van de melding.
- Als melder van het probleem houdt Z-CERT u op de hoogte van de voortgang van het oplossen van het probleem.
- In berichtgeving over het gemelde probleem zal OLVG, als u dit wenst, uw naam vermelden als de ontdekker.
- OLVG is een non-profit instelling en biedt daarom geen geldelijke beloning voor gemelde beveiligingsproblemen.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen. Samen overleggen wij daarna over de meerwaarde van een eventuele publicatie van het opgeloste probleem.

Met dank aan Floor Terra voor zijn voorbeeldtekst op http://responsibledisclosure.nl/

OLVG Coördinated Vulnerability Disclosure beleid

Publicatiedatum: 30-01-2023

OLVG Coördinated Vulnerability Disclosure beleid

Responsible Disclosure

At OLVG we work hard to maintain and improve the security of our (medical) devices, systems and services. No matter how much effort we put into system security, there might be vulnerabilities present. If you discover a vulnerability, you can report it safely via our *Coordinated Vulnerability Disclosure*, so OLVG can take safety measures.

Reporting a vulnerability

If you have found a vulnerability, we would like to hear about it so that we can take appropriate measures as quickly as possible. OLVG is keen to cooperate with you to protect our clients and systems better.

If you comply with our Coordinated Vulnerability Disclosure policy we have no reason to take legal action against you regarding the reported vulnerability. We ask you to:

- Make sure that your findings are in scope. On www.z-cert.nl/cvd-english/ you can check what is considered to be out-of-scope.
- Send your findings to Z-CERT. To do this please use the following mail template https://www.z-cert.nl/cvd-english/and send it to cvd@z-cert.nl encrypted with ZCERT's PGP-key. Z-CERT is an organization that handles all cyber security issues on behalf of OLVG. Z-CERT will work with you and OLVG to make sure that your report is handled with care.
- Provide adequate information to allow us to investigate and reproduce the vulnerability. Fill out every aspect of the CVD-form. This helps to resolve the problem as quickly as possible. An IP address or URL of the affected system with a description of the vulnerability will usually be sufficient, although more information might be necessary for more complex vulnerabilities. You may add a proof of concept as an attachment.
- Do not exploit vulnerabilities, e.g. by downloading more data than is needed to demonstrate the vulnerability, looking into third-party data, deleting or modifying data.
- If you suspect to have access to medical data we ask you to let us verify this.
- Do not share information on vulnerabilities until they have been resolved and erase any obtained data as soon as the problem is solved.
- Do not attack (physical) security using social engineering, distributed denial of service, spam, brute force attacks, third-party applications for instance, or other types of attacks.

How we will handle your report:

- OLVG and Z-CERT will treat your report confidentially and will not share your personal data unless required by law.
- Z-CERT will send you a confirmation of receipt and will respond within five working days with an evaluation of your report.
- OLVG and Z-CERT will keep you informed of the progress in resolving the problem.
- In communication about the reported problem, OLVG will mention your name as the discoverer if desired.
- OLVG is a non-profit organization and therefore does not offer monetary rewards for reported security vulnerabilities.

We strive to resolve any vulnerability as soon as possible. Once the problem has been resolved, we will decide in consultation whether and how details will be published.

With thanks to Floor Terra for his sample text in Dutch on http://responsiblediscloure.nl/

Publication date: 01-31-2023