Richtlinie zur Offenlegung von Sicherheitslücken

LivAssured BV / NightWatch verpflichtet sich zur Gewährleistung der Sicherheit und des Schutzes von Patienten und Kunden, die unsere Produkte und Dienstleistungen nutzen. Neben den neuesten Fortschritten in der Informationstechnologie gibt es auch zunehmende Risiken im Bereich der Sicherheit, wie z.B. Cyberangriffe, die Schwachstellen ausnutzen. LivAssured ist ein Unternehmen, das medizinische Geräte anbietet, die die Gesundheit und das Leben von Menschen mit Epilepsie betreffen. Wir sind bestrebt, unseren Kunden sichere medizinische Geräte sowie eine sichere Betriebsumgebung für unsere medizinischen Geräte zu bieten.

Wir möchten daher Kunden, Partner und Sicherheitsforscher, die unsere Werte teilen, ermutigen, in gutem Glauben jede digitale Schwachstelle zu melden, die sie entdecken. LivAssured schätzt die Bemühungen von Sicherheitsforschern und ihre Berichterstattung, da sie zur Verbesserung der Sicherheit und Zuverlässigkeit beitragen. Diese Richtlinie umreißt den Umfang und die abgedeckten Forschungen sowie den Prozess zur Meldung von Sicherheitslücken. Bitte beachten Sie, dass diese Richtlinie Änderungen unterliegt und daher regelmäßig überprüft werden sollte.

Umfang

Im Rahmen der LivAssured-Richtlinie zur Offenlegung von Sicherheitslücken sind die folgenden Produkte und Dienstleistungen eingeschlossen:

- Alle Varianten von NightWatch

- Andere von LivAssured entwickelte Produkte

- NightWatch-Domains und Subdomains:

  - *.nightwatchepilepsy.com

  - *.portal.nightwatchepilepsy.com

  - *.nightwatch.nl

Wenn Drittanbieterprodukte oder -dienstleistungen im Rahmen der Forschung betroffen sind, können wir keine Autorisierung für deren Testung erteilen. Bei Zweifeln fragen Sie bitte, bevor Sie ein digitales Asset, eine Anwendung oder eine Plattform testen.

Safe Harbor und Datenschutz

LivAssured verspricht, keine rechtlichen Schritte gegen Forscher einzuleiten oder zu unterstützen, die dieser Richtlinie folgen, während sie Sicherheitsforschungen durchführen. Dies gilt nicht, wenn erkennbar kriminelle oder nachrichtendienstliche Absichten verfolgt werden. Sollte ein Dritter rechtliche Schritte gegen einen Forscher einleiten, obwohl dieser gemäß dieser Richtlinie gehandelt hat, wird LivAssured sicherstellen, dass die Einhaltung der Richtlinie kommuniziert wird.

Forscher sollten LivAssured einen Bericht vorlegen, wenn sie Bedenken hinsichtlich der Einhaltung haben, bevor sie die Forschung fortsetzen. Diese Richtlinie befreit Forscher nicht von geltenden nationalen, föderalen, staatlichen und lokalen Gesetzen zu Hacking und Datenschutz.

Wir werden Ihren Bericht und Ihre persönlichen Daten vertraulich behandeln und nur insoweit weitergeben, wie es zur Behebung der Sicherheitslücke notwendig ist.

Richtlinien

Forscher mit guten Absichten und Zustimmung zu den Regeln verpflichten sich:

- Nur Geräte und Domains innerhalb des Geltungsbereichs der Richtlinie zu untersuchen.
- Unterbrechungen von Geräten oder Anwendungen zu vermeiden.
- Die Privatsphäre anderer zu respektieren, indem sie keine Daten zerstören, exfiltrieren, offenlegen oder auf andere Weise missbrauchen, die während der Forschung zugänglich werden könnten.
- Entdeckte Sicherheitslücken nicht auszunutzen; weiterführende Schritte wie Persistenz, laterale Bewegung, Datenexfiltration, Modifikation oder Löschung, Code-Uploads etc. sind nicht erlaubt.
- Sicherheitslücken nicht an Dritte weiterzugeben, es sei denn, dies ist vollständig mit LivAssured abgestimmt und schriftlich genehmigt.
- Keine Phishing-, Spam-, Social-Engineering- oder Denial-of-Service-Angriffe durchzuführen.
- Sicherheitslücken umgehend an LivAssured zu melden.

Meldeverfahren

Forscher sollten Sicherheitslücken an security@nightwatch.nl melden. LivAssured verpflichtet sich, den Eingang des Berichts für die im Geltungsbereich liegenden Geräte und Domains durch unser technisches Team zu bestätigen und dem Berichterstatter anschließend Feedback zu geben. Bitte beachten Sie, dass keine Erwartung auf Zahlung oder Entschädigung besteht und dass auf jegliche zukünftigen Ansprüche im Zusammenhang mit dem eingereichten Bericht verzichtet wird.

Durch die Einhaltung der folgenden Grundsätze können Sie die Wahrscheinlichkeit erhöhen, detailliertes Feedback zu Ihrem Bericht zu erhalten:

- Geben Sie vollständige Informationen zu den betroffenen Assets an.
- Reichen Sie einen Proof of Concept ein, der explizite Details zur Replikation der Sicherheitslücke enthält, einschließlich Zeitstempel und Screenshots des Problems.
- Erläutern Sie die potenziellen Auswirkungen und das Ausmaß der Sicherheitslücke.
- Verzichten Sie darauf, nur die Ausgabe automatisierter Tools einzureichen.

Dokumenttitel: Richtlinie zur Offenlegung von Sicherheitslücken

Revision: 2.0, 1. Juli 2024 16:28:13 (UTC/GMT +02:00 - Europa/Brüssel)