öffentlich

CEYONIQ Technology
A KYOCERA GROUP COMPANY

Richtlinie zur koordinierten Offenlegung von Schwachstellen

Coordinated Vulnerability Disclosure Policy der Ceyoniq Technology GmbH



© CEYONIQ Technology GmbH

CEYONIQ Technology
A KYOCERA GROUP COMPANY

INHALTSVERZEICHNIS

Inhaltsverzeichnis 2
1 Unser Anspruch 3
2 Geltungsbereich 3
3 Schwachstelle melden 3
4 Unser Vorgehen 4
5 Sicherheitshinweise und Veröffentlichung 4
6 Meldungen an Behörden 5
7 Komponenten von Drittanbietern 5
8 Änderungen dieser Richtlinie 5

1 UNSER ANSPRUCH

Unsere Kundinnen und Kunden vertrauen nscale geschäftskritische Dokumente und Informationen an. Die Sicherheit unserer Software hat für uns daher höchste Priorität. Trotz sorgfältiger Entwicklung und regelmäßiger Sicherheitstests können Schwachstellen nie vollständig ausgeschlossen werden. Wir begrüßen daher ausdrücklich Hinweise von Sicherheitsforschenden, Kunden, Partnern und allen anderen, die eine mögliche Schwachstelle entdeckt haben.

Diese Richtlinie beschreibt, wie Sie uns Schwachstellen melden, wie wir mit Ihrer Meldung umgehen und was Sie von uns erwarten können. Sie setzt die Anforderungen der Verordnung (EU) 2024/2847 (Cyber Resilience Act) an eine Richtlinie zur koordinierten Offenlegung von Schwachstellen um.

2 GELTUNGSBEREICH

Diese Richtlinie gilt für alle Produkte mit digitalen Elementen, die von der Ceyoniq Technology GmbH hergestellt und in Verkehr gebracht werden, insbesondere:

- nscale-Plattform und zugehörige Serverkomponenten
- nscale-Clients und -Apps (Web, Desktop, Mobile)
- Schnittstellen, Konnektoren und Integrationen (z. B. [SAP-, Microsoft-365-Integration])
- von Ceyoniq betriebene Cloud-Angebote
- die Websites unter ceyoniq.com und deren Subdomains

Informationen zu den unterstützten Produktversionen und deren Unterstützungszeitraum finden Sie in unserem Service-Portal. Details können Sie über unser Kontaktformular erfragen (https://ceyoniq.com/kontakt/).

Nicht erfasst sind Systeme unserer Kunden und Partner (auch wenn dort nscale betrieben wird), Dienste Dritter sowie kundenspezifische Anpassungen, die nicht von Ceyoniq entwickelt wurden. Für Tests an Kundeninstallationen benötigen Sie die Erlaubnis des jeweiligen Betreibers. Schwachstellen, die unser Produkt betreffen, können Sie uns aber selbstverständlich auch dann melden, wenn Sie sie in einer Kundenumgebung festgestellt haben.

3 SCHWACHSTELLE MELDEN

Bitte melden Sie Schwachstellen ausschließlich über folgende Kanäle:

- E-Mail: psirt@ceyoniq.com oder über https://ceyoniq.com/meldeformular/
- Verschlüsselung: Bitte verschlüsseln Sie vertrauliche Informationen mit unserem PGP-Schlüssel: https://ceyoniq.com/.well-known/security.txt
- Kunden und Partner können Sicherheitsprobleme auch direkt an den Ceyoniq Support melden und die entsprechenden Anfragen als sicherheitsrelevant kennzeichnen.

Damit wir Ihre Meldung zügig bearbeiten können, sind folgende Angaben hilfreich:

- betroffenes Produkt, Modul und Version sowie die Einsatzumgebung (z. B. Betriebssystem, Datenbank, On-Premises oder Cloud)
- Art der Schwachstelle und mögliche Auswirkungen
- nachvollziehbare Schritte zur Reproduktion oder ein Proof of Concept
- Ihre Einschätzung des Schweregrads, etwa nach CVSS
- ob Ihnen Hinweise auf eine aktive Ausnutzung vorliegen
- Kontaktdaten für Rückfragen und ob Sie in einem Sicherheitshinweis genannt werden möchten

Meldungen nehmen wir auf Deutsch oder Englisch entgegen. Anonyme Meldungen werden ebenfalls bearbeitet; Rückfragen sind dann allerdings nicht möglich.

4 UNSER VORGEHEN

Jede Meldung wird von unserem Product Security Team bearbeitet. In der Regel wird die Meldung nach folgendem Schema bearbeitet:

Schritt	Zeitrahmen
Kenntnisnahme des Eingangs	Innerhalb von 24 Stunden
Erste Einschätzung (Bestätigung, Schweregrad, weiteres Vorgehen)	Innerhalb von 72 Stunden
Abschlussbericht	Bei Schwachstellen 14 Tage nach der Bereitstellung der Korrektur, bei einem schwerwiegendem Sicherheitsvorfall einen Monat nach der 72 Stunden Frist
Bereitstellung einer Korrektur	So schnell wie möglich, priorisiert nach Schweregrad
Koordinierte Veröffentlichung	90 Tage nach der Bereitstellung einer Korrektur

Sicherheitsupdates stellen wir unverzüglich und für unsere Kunden kostenlos bereit, wo technisch möglich getrennt von Funktionsupdates. Updates werden über das Download-Portal der Ceyoniq bzw. die Container-Registry der Ceyoniq verteilt. Bis zur Verfügbarkeit einer Korrektur informieren wir betroffene Kunden, wenn nötig, über Maßnahmen zur Risikominderung.

Wird eine Schwachstelle aktiv ausgenutzt oder ist sie bereits öffentlich bekannt, handeln wir beschleunigt.

5 SICHERHEITSHINWEISE UND VERÖFFENTLICHUNG

Behobene Schwachstellen veröffentlichen wir in Sicherheitshinweisen in unserem Service-Portal. Diese enthalten eine Beschreibung der Schwachstelle, die betroffenen Produkte und Versionen, die Auswirkungen und den Schweregrad sowie Hinweise zur Behebung. Wo sinnvoll, vergeben wir CVE-Kennungen und stellen Sicherheitshinweise zusätzlich maschinenlesbar im Format CSAF bereit.

In begründeten Einzelfällen können wir die Veröffentlichung zurückstellen, wenn dies zum Schutz unserer Kunden erforderlich ist, bis diese die Möglichkeit hatten, das Update einzuspielen.

6 MELDUNGEN AN BEHÖRDEN

Wird eine Schwachstelle in unseren Produkten aktiv ausgenutzt oder kommt es zu einem schwerwiegenden Sicherheitsvorfall, der die Sicherheit unserer Produkte beeinträchtigt, erfüllen wir unsere Meldepflichten nach Art. 14 des Cyber Resilience Act. Die Meldung erfolgt über die zentrale Meldeplattform der ENISA an das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständigen CSIRT-Koordinator, mit einer Frühwarnung innerhalb von 24 Stunden, einer Meldung innerhalb von 72 Stunden und einem Abschlussbericht innerhalb der gesetzlichen Fristen. Betroffene Kunden informieren wir parallel über die Schwachstelle und die empfohlenen Maßnahmen.

7 KOMPONENTEN VON DRITTANBIETERN

nscale enthält Komponenten von Drittanbietern und Open-Source-Projekten. Diese erfassen wir in einer Software-Stückliste (SBOM). Betrifft eine Schwachstelle eine solche Komponente, informieren wir die für deren Wartung verantwortliche Stelle und teilen, sofern vorhanden, unsere Korrektur. Meldungen, die ausschließlich Produkte anderer Hersteller betreffen, leiten wir mit Ihrem Einverständnis an diese oder an das BSI weiter.

8 ÄNDERUNGEN DIESER RICHTLINIE

Wir überprüfen diese Richtlinie regelmäßig und passen sie bei Bedarf an. Maßgeblich ist die jeweils unter dieser Adresse veröffentlichte Fassung.

Kontakt: Ceyoniq Technology GmbH, Boulevard 9, 33613 Bielefeld, Deutschland, psirt@ceyoniq.com