Ordivis

TEIL VI · BETRIEB

Produktsicherheit & Meldewege

Schwachstellen melden, Aktualisierungen, sichere Ausserbetriebnahme

Produktversion 2026.09.20 · Handbuch-Revision 1.0
Stand 20.09.2026 · Plattform .NET 10 / Windows Server

ID-53 Produktsicherheit

Produktsicherheit & Meldewege

Dieses Kapitel enthält die Angaben nach **Anhang II der Cyberresilienz-Verordnung** (Verordnung (EU) 2024/2847). Es richtet sich an **IT-Betrieb** und an alle, die über die Beschaffung entscheiden. Die technische Installation steht in ID-50, die Härtung des Servers ebenfalls dort.

Dieselben Angaben stehen öffentlich unter ordivis.eu/produktsicherheit.html.

INHALT

1 Kontaktstelle für Schwachstellen

Melden Sie Schwachstellen an **security@ordivis.eu**. Das ist der einzige von uns benannte Meldeweg; maschinenlesbar steht er unter `https://ordivis.eu/.well-known/security.txt`.

Bitte veröffentlichen Sie Ihre Erkenntnisse nicht, solange eine Abhilfe aussteht. Unsere Strategie zur koordinierten Offenlegung, die Reaktionszeiten und die Zusage an gutgläubige Finder stehen auf der oben genannten Seite.

Ist eine Schwachstelle aktiv ausgenutzt, sind wir seit dem 11. September 2026 nach Artikel 14 der Verordnung verpflichtet, sie binnen 24 Stunden dem zuständigen Computer-Notfallteam und der ENISA zu melden. Wir unterrichten Sie dann ebenfalls — über die im Vertrag hinterlegte technische Anschrift. **Halten Sie diese Anschrift aktuell:** Sie ist der Weg, auf dem Sie von uns erfahren, dass Handlungsbedarf besteht.

2 Unterstützungszeitraum

Bis einschließlich 31. Dezember 2032. Bis zu diesem Zeitpunkt behandeln wir Schwachstellen und stellen Sicherheitsaktualisierungen **kostenlos** bereit. Der Zeitraum gilt für alle bis dahin ausgelieferten Fassungen und besteht unabhängig vom vereinbarten Supportmodell.

3 Sicherer Erstbetrieb

Ordivis ist für den Betrieb in einem verwalteten Firmennetz hinter einer Firewall vorgesehen, auf einem gepflegten Windows-Server mit PostgreSQL. Vor der Freigabe für Benutzer:

1. **Verschlüsselte Verbindung sicherstellen.** Im Auslieferungszustand läuft der Server in der Betriebsart `ReverseProxy` und erwartet, dass die Verschlüsselung **vorgelagert** abgeschlossen wird. Wird er ohne diese betrieben, laufen Anmeldedaten unverschlüsselt über das Netz. Alternativ die Betriebsart `Certificate` (eigenes Zertifikat) oder `Acme` (automatischer Bezug) einstellen — siehe ID-50.
2. **Erstkonto absichern.** Das beim Onboarding angelegte Konto erhält ein starkes Kennwort; Mehrfaktoranmeldung aktivieren (ID-41).
3. **Ungenutzte Module abschalten.** Jedes deaktivierte Modul ist eine Angriffsfläche weniger (ID-40).
4. **Erkennung mit eigenen Konten betreiben.** Für Netzscans eigene Konten mit den **geringsten ausreichenden Rechten** vergeben, keine Domänenadministratoren (Abschnitt 9).
5. **Datensicherung einrichten und einen Rücklauf prüfen** (ID-35). Eine Sicherung, die nie zurückgespielt wurde, ist eine Vermutung.

4 Sicherheitsaktualisierungen einspielen

Aktualisierungen werden über `https://ordivis.eu/updates` bereitgestellt. Jedes Paket trägt ein **signiertes Manifest**; der Aktualisierungsdienst prüft die Signatur vor dem Einspielen und bricht bei Abweichung ab.

- **Server:** Der Aktualisierungsvorgang ist in ID-50 beschrieben.
- **Arbeitsplätze:** Der Windows-Dienst `InfraDesk.ClientUpdate` vergleicht die installierte Fassung mit der bereitgestellten und spielt Aktualisierungen ein.

Prüfen Sie nach jeder Aktualisierung die Fassung unter **Über** in der Anwendung.

5 Selbsttätiges Einspielen abschalten

Sie können Aktualisierungen von Hand steuern. Halten Sie dazu den Dienst an und setzen Sie den Starttyp auf *Deaktiviert*:

```
Stop-Service InfraDesk.ClientUpdate
Set-Service  InfraDesk.ClientUpdate -StartupType Disabled
```

Zum Wiedereinschalten `-StartupType Automatic` setzen und den Dienst starten.

> **Was Sie damit übernehmen.** Ohne diesen Dienst erreichen Sie **auch Sicherheitsaktualisierungen nicht mehr selbsttätig**. Sie müssen dann selbst verfolgen, welche Fassungen erscheinen, und sie einspielen. Unsere Pflicht, sie bereitzustellen, bleibt bestehen — die Pflicht, sie anzuwenden, liegt dann vollständig bei Ihnen.

6 Auswirkungen von Änderungen auf Ihre Daten

- **Datenbankwanderungen** laufen beim Aktualisieren des Servers. Sie sind **nicht rückwärts** ausführbar: Ein Rücksprung auf eine ältere Fassung erfordert das Rückspielen einer Sicherung. **Vor jeder Aktualisierung sichern.**
- **Mandanten** liegen in getrennten Datenbanken. Das Löschen eines Mandanten entfernt dessen Datenbank vollständig.
- **Modulschalter** blenden Funktionen aus, **löschen aber keine Daten**. Ein später wieder eingeschaltetes Modul findet seinen Bestand vor.
- **Rechteänderungen** wirken sofort auf Lesen und Schreiben; bereits erzeugte Exporte und Berichte sind davon nicht berührt.

7 Sichere Außerbetriebnahme und Datenlöschung

Beim Rückbau einer Anlage sind **fünf** Orte zu räumen. Die Deinstallation über die Systemsteuerung entfernt die Dienste und Programmdateien — **die Daten bleiben absichtlich erhalten**, damit ein Rückbau nicht versehentlich zum Datenverlust wird.

1. **Dienste anhalten und entfernen:** `InfraDesk.API`, `InfraDesk.Portal`, `InfraDesk.ClientUpdate`, an entfernten Standorten `InfraDesk.Discovery.Collector`.
2. **Geplante Aufgaben entfernen:** `Ordivis-DailyBackup` und `Ordivis-Restore` (in Bestandsanlagen `InfraDesk-DailyBackup`, `InfraDesk-Restore`).
3. **Datenbanken löschen.** Je Mandant eine Datenbank, dazu die Verwaltungsdatenbank. Die PostgreSQL-Instanz heißt in Standardinstallationen `postgresql-ordivis`.
4. **Konfiguration und Sicherungen entfernen:** `%ProgramData%\InfraDesk` — darin liegen Konfiguration, hinterlegte Geheimnisse und, sofern nicht anders eingestellt, die Sicherungen.
5. **Protokolle entfernen.** ⚠️ **Die Protokolle liegen nicht zwingend unter `%ProgramData%`.** Ist in `%ProgramData%\InfraDesk\config\operations.json` ein abweichender Pfad hinterlegt, gilt dieser — er kann auf ein anderes Laufwerk zeigen. **Lesen Sie diese Datei, bevor Sie sie löschen**, sonst bleiben Protokolldaten zurück.

Auf den Arbeitsplätzen zusätzlich den Client deinstallieren und dessen lokales Benutzerprofilverzeichnis entfernen.

> **Sicheres Löschen.** Das Entfernen von Dateien und Datenbanken gibt den Speicher frei, überschreibt ihn aber nicht. Wo das gefordert ist — etwa bei Datenträgern, die das Haus verlassen — setzen Sie die Mittel Ihres Betriebssystems oder Ihrer Speicherplattform ein.

8 Stückliste der Fremdbestandteile

Jedem Installationspaket liegen im Programmverzeichnis bei:

Datei	Inhalt
`ordivis-sbom.cdx.json`	Maschinenlesbare Stückliste im Format **CycloneDX 1.6**
`THIRD-PARTY-NOTICES.txt`	Urhebervermerke und vollständige Lizenztexte

Die Stückliste nennt jeden ausgelieferten Fremdbestandteil mit Fassung, Lizenz und Verwendungszweck. Sie beantwortet die Frage, ob eine bekannt gewordene Schwachstelle in einer Fremdkomponente Ihre Anlage betrifft.

9 Bekannte Umstände, die zu erheblichen Risiken führen können

Anhang II Nummer 5 verlangt, solche Umstände zu benennen. Wir tun das vollständig.

- **Betrieb ohne vorgelagerte Verschlüsselung.** Siehe Abschnitt 3 Punkt 1. Der häufigste und folgenschwerste Fehler bei der Inbetriebnahme.
- **Die Erkennung speichert Anmeldedaten für Netzgeräte**, die häufig privilegiert sind. Wer Zugriff auf den Ordivis-Server erlangt, erlangt mittelbar Zugriff auf diese Daten.
- **Ordivis führt eine vollständige Abbildung Ihrer IT-Landschaft.** Ein unbefugter Lesezugriff ist deshalb für einen Angreifer ein Aufklärungsgewinn — auch ohne jede Schreibmöglichkeit.
- **Die Absicherung von Betriebssystem, Datenbank und Sicherungen liegt bei Ihnen.** Ordivis kann eine unsichere Umgebung nicht ausgleichen.

10 EU-Konformitätserklärung

Liegt noch nicht vor. Die Konformitätsbewertung nach der Cyberresilienz-Verordnung ist zum **11. Dezember 2027** fällig; die Erklärung wird zu diesem Zeitpunkt unter ordivis.eu/produktsicherheit.html veröffentlicht. Eine CE-Kennzeichnung für Cybersicherheit führt Ordivis IT bis dahin nicht.

11 Hersteller

Grams IT, Christian Grams, Mittelstraße 18, 34277 Fuldabrück, Deutschland. Allgemeine Anschrift **info@ordivis.eu**, Schwachstellen **security@ordivis.eu**.

Verwandte Themen

- **ID-50 – Betriebshandbuch – Installation & Serverbetrieb** – Sicherer Erstbetrieb und Härtung
- **ID-40 – Administrationshandbuch** – Aktualisierungen einspielen und Jobs steuern
- **ID-35 – Modul Datensicherung** – Sicherungen vor Änderungen und vor der Außerbetriebnahme
- **ID-02 – Systemvoraussetzungen & Architektur** – Komponenten und Netzwege des Produkts