SECURITY ADVISORY BOARD

IT-Service Walter

Jörn Walter
www.it-service-walter.com
15.10.2025

DAS SECURITY ADVISORY BOARD

ÜBERBLICK

DAS **SECURITY ADVISORY BOARD** IST EINE PROFESSIONELLE WINDOWS-DESKTOP-ANWENDUNG ZUR ÜBERWACHUNG, ANALYSE UND VERWALTUNG VON SICHERHEITSMELDUNGEN DES CERT-BUND (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). DIE ANWENDUNG BIETET IT-SICHERHEITSVERANTWORTLICHEN EINE ZENTRALE, ÜBERSICHTLICHE PLATTFORM ZUR ERFASSUNG UND BEWERTUNG AKTUELLER SICHERHEITSRISIKEN

Security Advisory Dashboard - Benutzerhandbuch

Inhaltsverzeichnis

1. Einführung

Was ist das Security Advisory Dashboard?

Das Security Advisory Dashboard ist eine Windows-Desktop-Anwendung zur Überwachung von Sicherheitsmeldungen des CERT-BUND (Computer Emergency Response Team des Bundesamtes für Sicherheit in der Informationstechnik). Die Anwendung hilft IT-Sicherheitsverantwortlichen dabei, Sicherheitsrisiken zu identifizieren, zu priorisieren und zu dokumentieren.

Systemvoraussetzungen

- **Betriebssystem**: Windows 10 oder höher
- **Framework**: .NET Framework 4.7.2 oder höher / .NET 8.0+
- **Internetverbindung**: Erforderlich für Datenabfrage
- **Bildschirmauflösung**: Mindestens 1920x1080

Installation

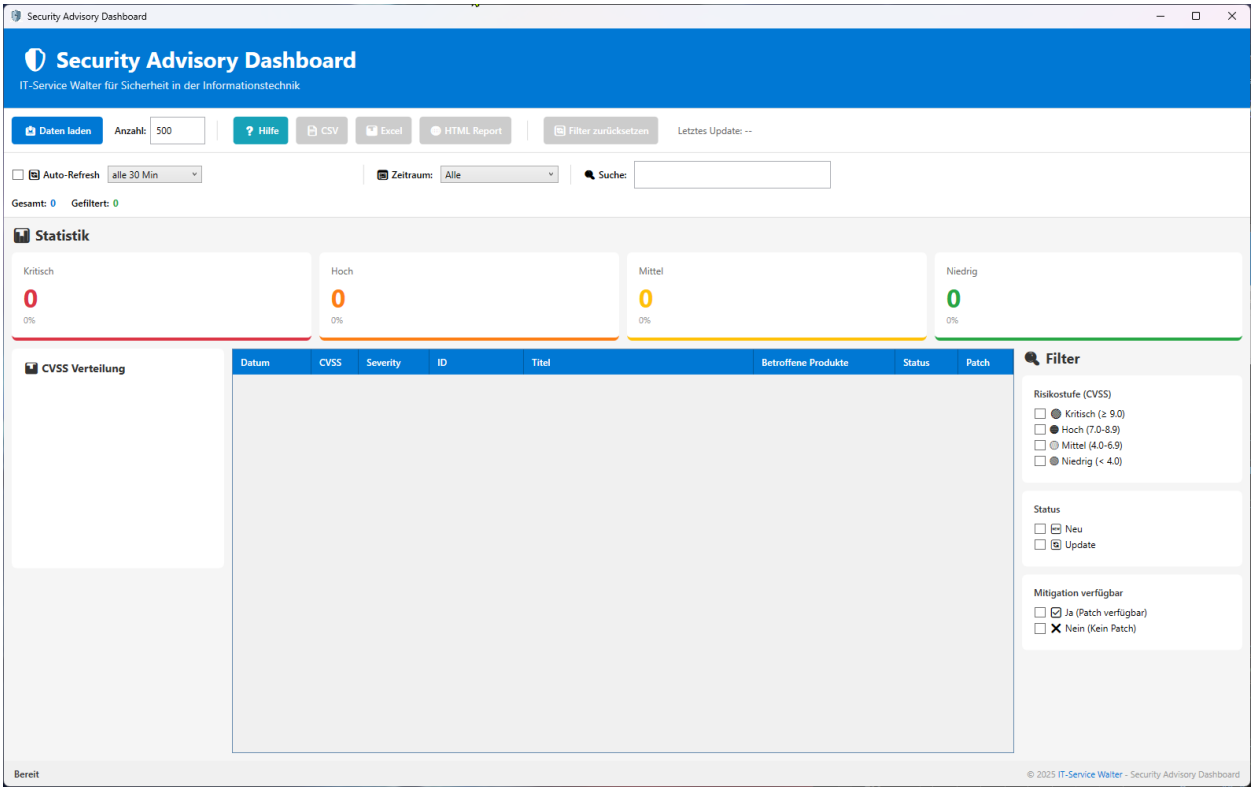
1. Entpacken Sie das Programm-Archiv in einen Ordner Ihrer Wahl
2. Starten Sie die Anwendung durch Doppelklick auf CertAdvisoryExtractor.exe
3. Keine weiteren Installationsschritte erforderlich, es sei denn Sie bekommen die Software mit einem integrierten Installer, der das Produkt lediglich entpackt

2. Erste Schritte

Programmstart

Nach dem Start der Anwendung sehen Sie die Hauptoberfläche mit folgenden Bereichen:

- **Header**: Zeigt den Programmnamen und Herausgeber
- **Toolbar**: Enthält Schaltflächen für Hauptfunktionen
- **Filter-Bereich**: Ermöglicht das Filtern von Daten
- **Hauptansicht**: Zeigt Statistiken, Diagramme und die Datentabelle
- **Statusleiste**: Informiert über den aktuellen Status

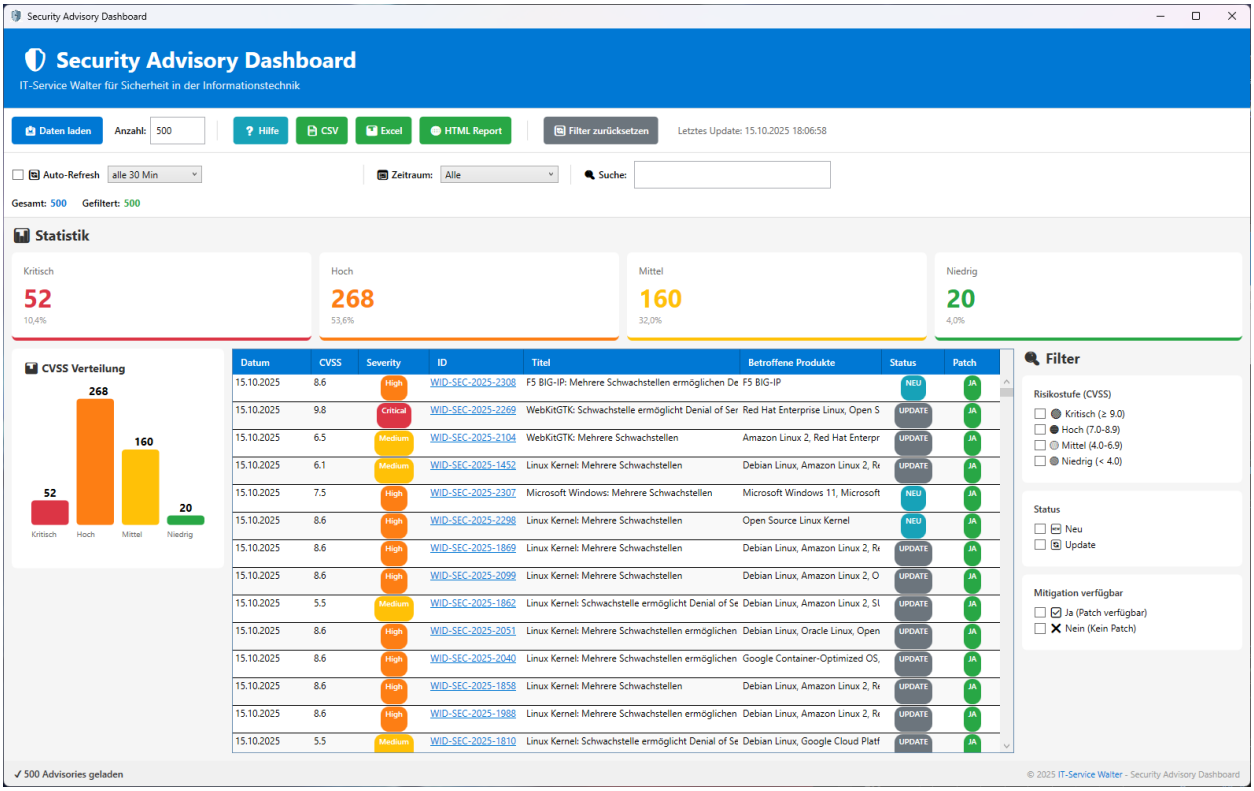


Erste Daten laden

Schritt-für-Schritt-Anleitung:

1. Klicken Sie auf die Schaltfläche "📥 **Daten laden**" in der Toolbar
2. Das Feld "Anzahl" zeigt standardmäßig 500 Einträge - dies kann angepasst werden
3. Ein Ladebildschirm erscheint und zeigt den Fortschritt
4. Nach Abschluss werden die Daten in der Tabelle angezeigt

Hinweis: Der erste Ladevorgang kann je nach Anzahl der gewählten Einträge 10-30 Sekunden dauern.



3. Benutzeroberfläche im Überblick

Header-Bereich

Der blaue Header-Bereich zeigt:

- **Programmtitel**: "Security Advisory Dashboard"
- **Untertitel**: "IT-Service Walter für Sicherheit in der Informationstechnik"

Toolbar (Werkzeugleiste)

Die Toolbar enthält folgende Schaltflächen:

- 📥 **Daten laden**: Lädt aktuelle Advisories von der CERT-BUND API
- **Anzahl-Feld**: Bestimmt die Anzahl der zu ladenden Einträge (1-5000)
- ❓ **Hilfe**: Öffnet das integrierte Hilfefenster
- 📄 **CSV**: Exportiert gefilterte Daten als CSV-Datei
- 📊 **Excel**: Exportiert gefilterte Daten als formatierte Excel-Datei
- 🌐 **HTML Report**: Erstellt einen umfassenden HTML-Bericht
- 🔄 **Filter zurücksetzen**: Setzt alle aktiven Filter zurück
- **Letztes Update**: Zeigt Datum und Uhrzeit der letzten Datenaktualisierung

Filter-Bereich

Der Filter-Bereich ist in zwei Zeilen unterteilt:

Erste Zeile:

- Auto-Refresh Einstellungen
- Zeitraum-Filter
- Suchfeld

Zweite Zeile:

- Anzahl-Anzeigen (Gesamt / Gefiltert)

Hauptansicht

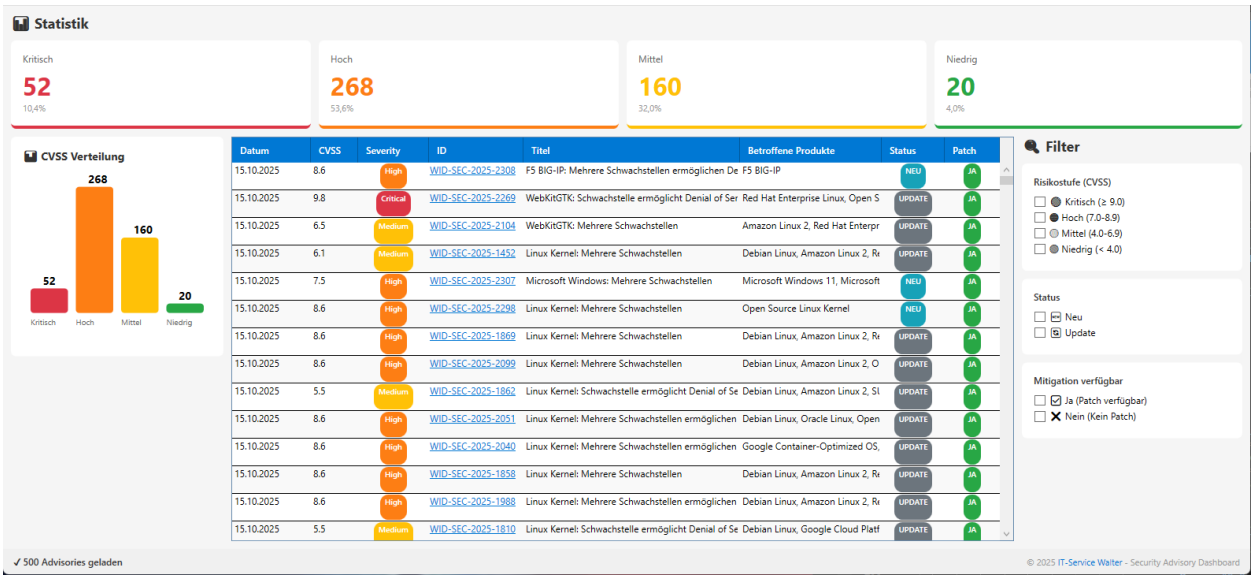
Die Hauptansicht besteht aus drei Bereichen:

Statistik-Cards (oben):

- Zeigt Anzahl und Prozentsatz für jede Risikostufe
- Farbcodiert: Rot (Kritisch), Orange (Hoch), Gelb (Mittel), Grün (Niedrig)

Drei-Spalten-Layout:

1. **Links**: CVSS-Verteilungsdiagramm (Balkendiagramm)
2. **Mitte**: Datentabelle mit Sicherheitsmeldungen
3. **Rechts**: Detaillierte Filteroptionen



Statusleiste

Die Statusleiste am unteren Rand zeigt:

- **Links**: Aktuelle Statusmeldungen und Erfolgsmeldungen
- **Rechts**: Copyright-Informationen und Link zur Webseite

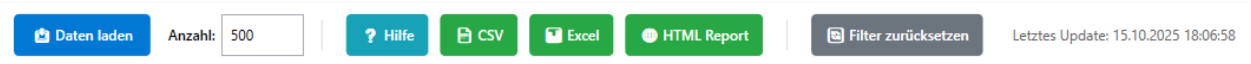
4. Daten laden und aktualisieren

Anzahl der zu ladenden Einträge festlegen

Standard: 500 Einträge **Maximum**: 5000 Einträge

So ändern Sie die Anzahl:

1. Klicken Sie in das Feld "Anzahl" in der Toolbar
2. Geben Sie die gewünschte Zahl ein (1-5000)
3. Drücken Sie Enter oder klicken Sie auf "Daten laden"



Empfehlungen:

- **Schnelle Übersicht**: 200-500 Einträge
- **Umfassende Analyse**: 1000-2000 Einträge
- **Vollständiges Archiv**: 3000-5000 Einträge

Manuelles Laden von Daten

1. Klicken Sie auf **" 📥 Daten laden"**
2. Warten Sie, bis der Ladevorgang abgeschlossen ist
3. Die Statusleiste zeigt: "✓ [Anzahl] Advisories geladen"

Ladefortschritt verstehen

Während des Ladevorgangs sehen Sie:

- Ein halbtransparentes Overlay mit Ladeanimation
- Fortschrittsanzeige: "Lade Seite X... (Y/Z)"
- Die Meldung " ⏳ Laden..." im Overlay

Hinweis: Das Laden erfolgt seitenweise (100 Einträge pro Seite) mit kurzen Pausen zwischen den Anfragen, um die API nicht zu überlasten.

5. Auto-Refresh konfigurieren

Was ist Auto-Refresh?

Die Auto-Refresh-Funktion lädt automatisch in regelmäßigen Abständen neue Daten von der CERT-BUND API. Dies ist besonders nützlich für kontinuierliche Überwachung.

Auto-Refresh aktivieren

Schritt-für-Schritt:

1. Wählen Sie ein Intervall aus dem Dropdown-Menü:
    - **alle 5 Min** (für kritische Überwachung)
    - **alle 30 Min** (für aktive Überwachung)
    - **jede Stunde** (Standard-Überwachung)
    - **alle 4 Std** (regelmäßige Updates)
2. Aktivieren Sie die Checkbox "**Auto-Refresh**"
3. Der Countdown beginnt und zeigt die verbleibende Zeit bis zum nächsten Update

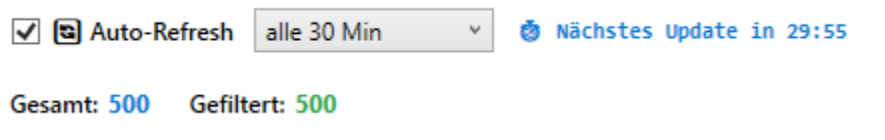
Auto-Refresh deaktivieren

- Deaktivieren Sie die Checkbox "**Auto-Refresh**"
- Der Timer wird gestoppt
- Die Statusleiste zeigt: "Auto-Refresh deaktiviert"

Countdown-Anzeige verstehen

Die Countdown-Anzeige zeigt:

- **Format bei über 1 Stunde**: ⏱ Nächstes Update in HH:MM:SS
- **Format unter 1 Stunde**: ⏱ Nächstes Update in MM:SS
- **Während des Updates**: ⏱ Update läuft...



Beispiel: ⏱ Nächstes Update in 27:45 bedeutet 27 Minuten und 45 Sekunden bis zum nächsten automatischen Update.

Best Practices für Auto-Refresh

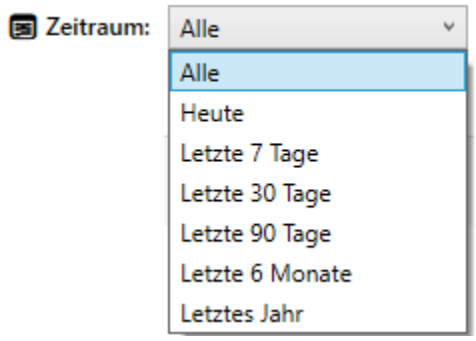
- **5 Minuten**: Nur während akuter Bedrohungslagen
- **30 Minuten**: Für aktives Monitoring während der Arbeitszeit
- **1 Stunde**: Empfohlene Standardeinstellung
- **4 Stunden**: Für Hintergrundüberwachung ohne aktive Nutzung

Achtung: Sehr kurze Intervalle (5 Min) erzeugen mehr API-Anfragen und Systemlast.

6. Filter und Suche verwenden

Zeitraum-Filter

Mit dem Zeitraum-Filter können Sie Advisories nach Veröffentlichungsdatum filtern.



Verfügbare Zeiträume:

- **Alle**: Keine zeitliche Einschränkung
- **Heute**: Nur heute veröffentlichte Advisories
- **Letzte 7 Tage**: Aktuelle Woche
- **Letzte 30 Tage**: Aktueller Monat
- **Letzte 90 Tage**: Aktuelles Quartal
- **Letzte 6 Monate**: Halbjahr
- **Letztes Jahr**: 12 Monate

Anwendung:

1. Klicken Sie auf das Dropdown-Menü "**Zeitraum**"
2. Wählen Sie den gewünschten Zeitraum
3. Die Tabelle wird automatisch aktualisiert

Volltext-Suche

Das Suchfeld durchsucht folgende Felder:

- **Titel** der Advisory
- **ID** (z.B. WID-SEC-2024-0001)
- **Betroffene Produkte**

Verwendung:

1. Geben Sie einen Suchbegriff in das Feld **"🔍 Suche"** ein
2. Die Filterung erfolgt automatisch während der Eingabe
3. Groß-/Kleinschreibung wird nicht beachtet

Beispiele:

- Windows - Zeigt alle Advisories zu Windows-Produkten
- CVE-2024 - Zeigt alle Advisories mit dieser CVE-Nummer
- Microsoft - Zeigt alle Microsoft-bezogenen Meldungen

CVSS-Risikostufen-Filter

Filtern Sie nach Schweregrad der Sicherheitslücken:

Filter-Optionen:

- 🔴 **Kritisch (≥ 9.0)**: CVSS-Score 9.0 bis 10.0
- 🟠 **Hoch (7.0-8.9)**: CVSS-Score 7.0 bis 8.9
- 🟡 **Mittel (4.0-6.9)**: CVSS-Score 4.0 bis 6.9
- 🟢 **Niedrig (< 4.0)**: CVSS-Score unter 4.0

Anwendung:

1. Aktivieren Sie eine oder mehrere Checkboxen im Filter-Bereich rechts
2. Die Tabelle zeigt nur Einträge mit den gewählten Risikostufen
3. Mehrfachauswahl ist möglich (UND-Verknüpfung)

Beispiel: Aktivieren Sie "Kritisch" und "Hoch" für prioritäre Sicherheitslücken.

Status-Filter

Filtern Sie nach dem Status der Advisory:

- 🆕 **Neu**: Erstveröffentlichung
- 🔄 **Update**: Aktualisierung einer bestehenden Advisory

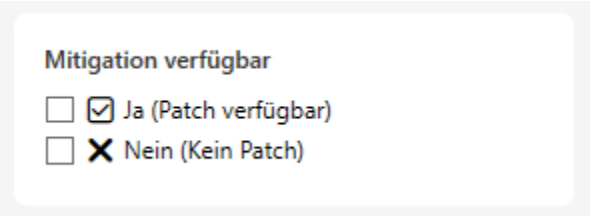
Verwendung:

1. Wählen Sie im rechten Filter-Bereich "Status"
2. Aktivieren Sie "Neu" für neue Meldungen
3. Aktivieren Sie "Update" für aktualisierte Meldungen

Mitigation-Filter

Zeigt an, ob ein Sicherheitspatch verfügbar ist:

- ✅ **Ja (Patch verfügbar)**: Hersteller hat einen Patch bereitgestellt
- ❌ **Nein (Kein Patch)**: Noch kein Patch verfügbar



Wichtig: Advisories ohne Patch erfordern alternative Schutzmaßnahmen (Workarounds, Härtungsmaßnahmen).

Filter kombinieren

Alle Filter können kombiniert werden für präzise Ergebnisse:

Beispiel-Szenario: "Zeige mir alle kritischen Windows-Sicherheitslücken der letzten 7 Tage ohne verfügbaren Patch"

Filtereinstellungen:

1. Zeitraum: "Letzte 7 Tage"
2. Suche: "Windows"
3. Risikostufe: "Kritisch" ✓
4. Mitigation: "Nein" ✓

Filter zurücksetzen

Klicken Sie auf **" 🔄 Filter zurücksetzen"**, um:

- Alle Checkboxen zu deaktivieren
- Das Suchfeld zu leeren
- Den Zeitraum auf "Alle" zu setzen
- Die vollständige Datenmenge anzuzeigen

Die Statusleiste zeigt: "✓ Alle Filter zurückgesetzt"

7. Daten analysieren und verstehen

Statistik-Cards interpretieren

Die vier Statistik-Cards oben zeigen:

Kritisch (Rot)

- Anzahl der kritischen Sicherheitslücken
- Prozentsatz an allen Advisories
- **Bedeutung**: Höchste Priorität, sofortiges Handeln erforderlich

Hoch (Orange)

- Anzahl der Schwachstellen mit hohem Risiko
- Prozentsatz an allen Advisories
- **Bedeutung**: Hohe Priorität, zeitnahes Patchen (innerhalb Tage)

Mittel (Gelb)

- Anzahl mittelschwerer Sicherheitslücken
- Prozentsatz an allen Advisories
- **Bedeutung**: Moderate Priorität, regulärer Patch-Zyklus

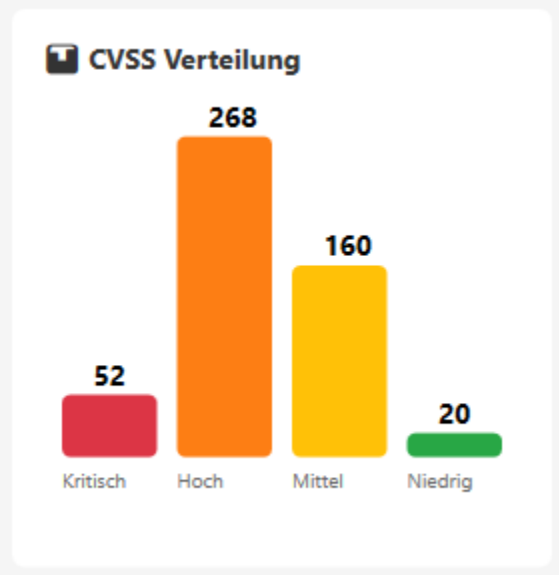
Niedrig (Grün)

- Anzahl geringfügiger Schwachstellen
- Prozentsatz an allen Advisories
- **Bedeutung**: Niedrige Priorität, routinemäßige Wartung

CVSS-Verteilungsdiagramm lesen

Das Balkendiagramm links zeigt die Verteilung der Risikostufen visuell:

- **Höhe der Balken**: Relative Anzahl in jeder Kategorie
- **Zahl auf dem Balken**: Absolute Anzahl
- **Farbe**: Entspricht der Risikostufe



Interpretation:

- Hohe rote/orange Balken = Viele kritische Bedrohungen
- Hohe grüne Balken = Überwiegend unkritische Meldungen

Datentabelle verstehen

Die Haupttabelle enthält folgende Spalten:

Datum

- Veröffentlichungsdatum der Advisory
- Format: TT.MM.JJJJ

CVSS

- Common Vulnerability Scoring System Score
- Bereich: 0.0 bis 10.0
- Je höher, desto kritischer

Severity

- Farbcodiertes Badge (Critical/High/Medium/Low)
- Basiert auf CVSS-Score

ID

- Eindeutige CERT-BUND Kennung
- Klickbarer Link zur vollständigen Advisory
- Format: WID-SEC-JJJJ-NNNN

Titel

- Beschreibung der Sicherheitslücke
- Enthält oft betroffene Produkte und Art der Schwachstelle

Betroffene Produkte

- Liste der betroffenen Software/Hardware
- Bei mehr als 3 Produkten: "+X" für weitere

Status

- NEU (türkis): Erstveröffentlichung
- UPDATE (grau): Aktualisierung

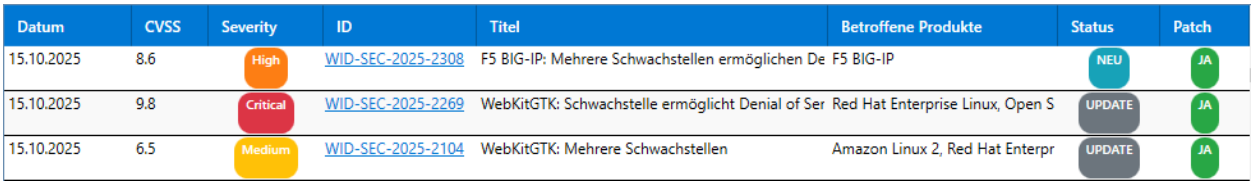
Patch

- JA (grün): Sicherheitspatch verfügbar
- NEIN (rot): Kein Patch verfügbar

Advisory-Details aufrufen

So öffnen Sie die vollständige Advisory:

1. Klicken Sie auf die **ID** (blaue, unterstrichene Nummer) in der Tabelle



Datum	CVSS	Severity	ID	Titel	Betroffene Produkte	Status	Patch
15.10.2025	8.6	High	WID-SEC-2025-2308	F5 BIG-IP: Mehrere Schwachstellen ermöglichen De	F5 BIG-IP	NEU	JA
15.10.2025	9.8	Critical	WID-SEC-2025-2269	WebKitGTK: Schwachstelle ermöglicht Denial of Ser	Red Hat Enterprise Linux, Open S	UPDATE	JA
15.10.2025	6.5	Medium	WID-SEC-2025-2104	WebKitGTK: Mehrere Schwachstellen	Amazon Linux 2, Red Hat Enterpr	UPDATE	JA

2. Ihr Standard-Browser öffnet die CERT-BUND-Webseite
3. Dort finden Sie:
    - Vollständige Beschreibung
    - Betroffene Versionen
    - Lösungsmaßnahmen
    - CVE-Nummern
    - Referenzen und Links

Sortierung nutzen

Klicken Sie auf einen **Spalten-Header**, um die Tabelle zu sortieren:

Datum	CVSS	Severity	ID	Titel	Betroffene Produkte	Status	Patch

- **Erster Klick**: Aufsteigend sortieren
- **Zweiter Klick**: Absteigend sortieren
- **Dritter Klick**: Sortierung aufheben

Nützliche Sortierungen:

- Nach **Datum**: Neueste Meldungen zuerst
- Nach **CVSS**: Kritischste zuerst
- Nach **Titel**: Alphabetische Übersicht

8. Export-Funktionen nutzen

CSV-Export

Der CSV-Export eignet sich für:

- Weiterverarbeitung in Excel/LibreOffice
- Import in andere Systeme
- Skript-basierte Verarbeitung

Durchführung:

1. Wenden Sie gewünschte Filter an
2. Klicken Sie auf **" CSV"**
3. Wählen Sie Speicherort und Dateinamen
4. Standardname: CERT_Advisories_JJJJMMTT_HHMMSS.csv
5. Klicken Sie auf "Speichern"

CSV-Format:

- **Trennzeichen**: Semikolon (;)
- **Encoding**: UTF-8
- **Spalten**: Datum, CVSS, Severity, ID, Titel, Betroffene Produkte, Status, Mitigation, URL

Hinweis: Nur gefilterte Daten werden exportiert!

Excel-Export

Der Excel-Export bietet:

- Professionelle Formatierung
- Farbcodierte Risikostufen
- Klickbare URLs
- Spalten-Anpassung

Durchführung:

1. Wenden Sie gewünschte Filter an
2. Klicken Sie auf **" 📊 Excel"**
3. Wählen Sie Speicherort und Dateinamen
4. Standardname: CERT_Advisories_JJJJMMTT_HHMMSS.xlsx
5. Klicken Sie auf "Speichern"

Excel-Features:

- **Formatierte Überschriften**: Blauer Hintergrund, weiße Schrift
- **Farbcodierung**:
    - Kritisch: Roter Hintergrund
    - Hoch: Oranger Hintergrund
    - Mittel: Gelber Hintergrund
    - Niedrig: Grüner Hintergrund
- **Hyperlinks**: URLs sind direkt anklickbar
- **Auto-Anpassung**: Spaltenbreiten optimiert

Verwendungszwecke:

- Management-Reports
- Präsentationen
- Archivierung
- Weitergabe an Kollegen

HTML-Report Export

Der HTML-Report ist der umfangreichste Export und enthält:

- Vollständige Statistiken
- Erklärung der CVSS-Risikostufen
- Professionelles Design
- Druckoptimierung

Durchführung:

1. Wenden Sie gewünschte Filter an
2. Klicken Sie auf **" HTML Report"**
3. Wählen Sie Speicherort und Dateinamen
4. Standardname: CERT_Advisory_Report_JJJJMMTT_HHMMSS.html
5. Klicken Sie auf "Speichern"
6. Optional: Direkt im Browser öffnen (Ja/Nein-Abfrage)

Report-Struktur:

1. **Header**: Titel und Untertitel
2. **Meta-Informationen**: Erstellungsdatum, Anzahl Einträge, Quelle
3. **Statistik-Cards**: Anzahl je Risikostufe
4. **Risikostufen-Erklärung**: Detaillierte Beschreibung von CVSS
5. **Datentabelle**: Alle gefilterten Advisories
6. **Footer**: Copyright und Quelle

Besonderheiten:

- **Responsive Design**: Passt sich verschiedenen Bildschirmgrößen an
- **Druckoptimierung**: Sauberer Ausdruck möglich
- **Standalone**: Funktioniert ohne Internetverbindung

- **Professionelles Layout**: Geeignet für Management-Präsentationen

Verwendungszwecke:

- Audit-Dokumentation
- Compliance-Nachweise
- Management-Berichte
- Weitergabe per E-Mail
- Archivierung

Export-Best-Practices

Vor dem Export:

1. Filter korrekt setzen (nur relevante Daten exportieren)
2. Zeitraum eingrenzen für spezifische Analysen
3. Bei großen Datenmengen: Mehrere Exporte mit verschiedenen Filtern

Dateinamen-Konvention:

- Standardnamen enthalten Datum und Uhrzeit
- Passen Sie Namen bei Bedarf an (z.B. "CERT_Q1_2024_Kritisch.xlsx")

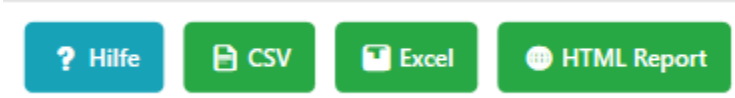
Regelmäßigkeit:

- Wöchentliche Exporte für Trend-Analysen
- Monatliche Reports für Management
- Ad-hoc Exporte bei Incidents

9. Hilfe und Support

Integrierte Hilfe aufrufen

1. Klicken Sie auf **" ❓ Hilfe"** in der Toolbar



2. Ein neues Fenster öffnet sich mit:
    - Erklärung der CVSS-Risikostufen
    - Beschreibung der Hauptfunktionen
    - Tipps zur Nutzung

CVSS-Score verstehen

CVSS (Common Vulnerability Scoring System):

Ein standardisiertes Bewertungssystem für Sicherheitslücken (0.0 - 10.0)

Bewertungsfaktoren:

- Ausnutzbarkeit (Attack Complexity)
- Erforderliche Privilegien (Privileges Required)
- Benutzerinteraktion (User Interaction)
- Auswirkungen auf Vertraulichkeit (Confidentiality Impact)
- Auswirkungen auf Integrität (Integrity Impact)
- Auswirkungen auf Verfügbarkeit (Availability Impact)

Einteilung:

- **Kritisch (9.0-10.0)**: Sofortiges Handeln erforderlich
    - Einfach ausnutzbar
    - Schwerwiegende Auswirkungen
    - Oft bereits aktiv im Einsatz
    - Beispiel: Remote Code Execution ohne Authentifizierung
- **Hoch (7.0-8.9)**: Hohe Priorität
    - Leicht ausnutzbar oder schwere Auswirkungen
    - Kann zu Systemkompromittierung führen
    - Beispiel: Privilege Escalation
- **Mittel (4.0-6.9)**: Moderate Priorität
    - Mittlere Komplexität oder lokaler Zugriff erforderlich
    - Begrenzte Auswirkungen
    - Beispiel: Information Disclosure

- **Niedrig (0.1-3.9)**: Geringe Priorität
    - Schwer ausnutzbar
    - Minimale Auswirkungen
    - Beispiel: Client-side Denial of Service

Statusmeldungen verstehen

Toolbar-Statusmeldungen:

- "Bereit" - Anwendung wartet auf Eingabe
- "Lade Daten von CERT-BUND API..." - Ladevorgang läuft
- "Lade Seite X... (Y/Z)" - Fortschritt beim Laden
- "✓ X Advisories geladen" - Laden erfolgreich abgeschlossen
- "✓ Auto-Refresh aktiviert (alle X)" - Auto-Refresh aktiv
- "Auto-Refresh deaktiviert" - Auto-Refresh gestoppt
- "✓ CSV exportiert: X Einträge" - Export erfolgreich
- "✓ Excel exportiert: X Einträge" - Export erfolgreich
- "✓ HTML Report exportiert: X Einträge" - Export erfolgreich
- "✓ Alle Filter zurückgesetzt" - Filter wurden zurückgesetzt
- "❌ Fehler beim Laden der Daten" - Fehler aufgetreten

Overlay-Meldungen:

- "⏳ Laden..." - Hauptmeldung während des Ladens
- "Bitte warten..." - Hinweis auf laufenden Prozess

10. Best Practices

Empfohlener Workflow für tägliches Monitoring

Morgens (Arbeitsbeginn):

1. Programm starten
2. Auto-Refresh aktivieren (1 Stunde)
3. Filter setzen:
    - Zeitraum: "Letzte 24 Stunden"
    - Risikostufe: "Kritisch" + "Hoch"
4. Neue kritische Advisories prüfen
5. Bei Bedarf: HTML-Report erstellen

Während des Tages:

- Programm im Hintergrund laufen lassen
- Auto-Refresh überwacht kontinuierlich
- Bei neuen kritischen Meldungen: Sofort reagieren

Abends (Tagesabschluss):

- Excel-Export der Tages-Advisories
- Filter zurücksetzen
- Programm beenden

Strategien für verschiedene Szenarien

Akute Bedrohungslage:

1. Auto-Refresh auf 5-30 Minuten setzen
2. Filter: "Kritisch" + eigene Produktumgebung (z.B. "Windows")
3. Mitigation-Filter: "Nein" (keine Patches) aktivieren
4. Sofort-Maßnahmen prüfen (Workarounds, Firewallregeln)

Patch-Management-Planung:

1. Zeitraum: "Letzte 30 Tage"
2. Filter: "Hoch" + "Kritisch"
3. Mitigation: "Ja" (Patches verfügbar)
4. Excel-Export für Patch-Priorisierung
5. Nach Produkt sortieren

Compliance-Reporting:

1. Zeitraum: Berichtszeitraum wählen (z.B. Quartal)
2. Alle Filter deaktivieren (vollständige Übersicht)
3. HTML-Report erstellen
4. Zusätzlich Excel für detaillierte Auswertung

Trend-Analyse:

1. Mehrere Exporte über verschiedene Zeiträume
2. Vergleich der Statistiken
3. Entwicklung der Risikostufen beobachten

Ressourcen-Management

Für bessere Performance:

- Bei großen Datenmengen (>2000): Regelmäßig Programm neu starten
- Auto-Refresh bei Nicht-Nutzung deaktivieren
- Nicht benötigte Daten durch Filter ausblenden

Netzwerk-Schonung:

- Auto-Refresh nicht unter 30 Minuten setzen (außer Notfälle)
- Laden von maximal 1000-2000 Einträgen für normale Arbeit
- 5000 Einträge nur für umfassende Analysen

Datensicherheit und Datenschutz

- Exportierte Dateien enthalten ggf. sensible Informationen über Ihre IT-Infrastruktur
- Speichern Sie Exporte an sicheren Orten
- HTML-Reports vor Weitergabe prüfen (ggf. Filter anwenden)
- Regelmäßige Löschung alter Export-Dateien

11. Häufig gestellte Fragen (FAQ)

Allgemeine Fragen

F: Wie aktuell sind die Daten? A: Die Daten werden in Echtzeit von der CERT-BUND API abgerufen. Beim Laden erhalten Sie immer die neuesten verfügbaren Advisories.

F: Werden die Daten lokal gespeichert? A: Nein, die Daten werden bei jedem Start neu geladen. Sie können jedoch Exporte erstellen zur Archivierung.

F: Kann ich mehrere Instanzen gleichzeitig laufen lassen? A: Ja, das ist möglich, aber nicht empfohlen (erhöhte Netzwerklast).

F: Benötige ich einen API-Key für CERT-BUND? A: Nein, die CERT-BUND API ist öffentlich zugänglich und erfordert keine Authentifizierung.

Funktionsfragen

F: Warum werden nicht alle Advisories geladen? A: Die Anzahl wird durch das Feld "Anzahl" begrenzt. Erhöhen Sie den Wert für mehr Einträge (max. 5000).

F: Kann ich eigene Filter-Kombinationen speichern? A: Aktuell nicht. Dies ist eine mögliche zukünftige Funktion.

F: Warum zeigt der CVSS-Score manchmal 0.0? A: Bei sehr neuen Advisories liegt manchmal noch keine CVSS-Bewertung vor.

F: Kann ich die Spaltenbreiten in der Tabelle anpassen? A: Ja, ziehen Sie die Spalten-Trennlinien mit der Maus.

F: Was bedeutet "+3" bei betroffenen Produkten? A: Es gibt 3 weitere betroffene Produkte. Klicken Sie auf die ID für die vollständige Liste.

Export-Fragen

F: Werden beim Export auch die Filter berücksichtigt? A: Ja, alle Exporte berücksichtigen die aktiven Filter. Es werden nur die sichtbaren Daten exportiert.

F: Kann ich das Excel-Format anpassen? A: Das Format ist vordefiniert. Sie können die Excel-Datei nach dem Export manuell anpassen.

F: Warum kann ich den HTML-Report nicht im Browser öffnen? A: Möglicherweise blockiert ein Sicherheitsprogramm. Öffnen Sie die Datei manuell aus dem Explorer.

F: Kann ich Exporte automatisieren? A: Aktuell nicht über die GUI. Dies wäre mit Scripting möglich (zukünftige Funktion).

Auto-Refresh-Fragen

F: Läuft Auto-Refresh auch wenn das Fenster minimiert ist? A: Ja, solange das Programm läuft, funktioniert Auto-Refresh.

F: Wie viele Daten werden bei Auto-Refresh geladen? A: Die Anzahl aus dem "Anzahl"-Feld. Es werden alle Einträge neu geladen.

F: Verliere ich meine Filter bei Auto-Refresh? A: Nein, alle Filter bleiben aktiv und werden auf die neuen Daten angewendet.

Technische Fragen

F: Welche Ports nutzt die Anwendung? A: Standard HTTPS (Port 443) für die API-Kommunikation.

F: Funktioniert die App hinter einem Proxy? A: Ja, wenn Ihr System korrekt für Proxy konfiguriert ist.

F: Kann ich die App auf einem USB-Stick laufen lassen? A: Ja, die Anwendung ist portabel und benötigt keine Installation.

F: Wo werden Einstellungen gespeichert? A: Aktuell werden keine Einstellungen persistent gespeichert. Beim nächsten Start sind alle Filter zurückgesetzt.

12. Fehlerbehebung

Häufige Fehler und Lösungen

Problem: "Fehler beim Laden der Daten"

Mögliche Ursachen und Lösungen:

1. **Keine Internetverbindung**
    - Lösung: Internetverbindung prüfen
    - Testen: Browser öffnen und beliebige Webseite aufrufen
2. **Firewall blockiert Zugriff**
    - Lösung: Ausnahmeregel für die Anwendung erstellen
    - Alternativ: Temporär Firewall deaktivieren zum Testen
3. **CERT-BUND API nicht erreichbar**
    - Lösung: Später erneut versuchen (Wartungsarbeiten möglich)
    - Prüfen: https://wid.cert-bund.de im Browser aufrufen
4. **Timeout bei großer Anzahl**
    - Lösung: Anzahl der Einträge reduzieren (z.B. 500 statt 5000)
    - Mehrere kleinere Ladevorgänge durchführen

Problem: Auto-Refresh funktioniert nicht

Lösungen:

1. Intervall neu auswählen
2. Checkbox aus- und wieder einschalten
3. Programm neu starten

Problem: Export-Fehler

CSV/Excel/HTML-Export schlägt fehl:

1. **Speicherort nicht beschreibbar**
    - Lösung: Anderen Speicherort wählen (z.B. Desktop)
    - Administratorrechte prüfen
2. **Datei bereits geöffnet**
    - Lösung: Vorherige Export-Datei schließen
    - Anderen Dateinamen wählen
3. **Nicht genügend Speicherplatz**
    - Lösung: Speicherplatz freigeben
    - Weniger Einträge exportieren (Filter setzen)
4. **Excel-Export: ClosedXML-Fehler**
    - Lösung: .NET Framework aktualisieren
    - Notlösung: CSV-Export verwenden

Problem: Programm reagiert nicht / stürzt ab

Sofort-Maßnahmen:

1. Task-Manager öffnen (Strg+Shift+Esc)
2. Prozess "CertAdvisoryExtractor" beenden
3. Programm neu starten

Vermeidung:

- Nicht zu viele Daten laden (max. 2000 für normale Arbeit)
- Auto-Refresh nicht zu aggressiv einstellen
- Bei Problemen: Programm regelmäßig neu starten

Problem: Darstellungsfehler

Tabelle wird nicht korrekt angezeigt:

1. Fenster maximieren
2. Programm neu starten
3. Bildschirmauflösung prüfen (min. 1280x800)

Statistiken fehlen:

- Daten laden durchführen
- Filter überprüfen (eventuell keine Daten im Filter)

Problem: Links funktionieren nicht

ID-Links öffnen keine Webseite:

1. Standard-Browser prüfen
2. Browser manuell öffnen und URL kopieren
3. Sicherheitssoftware prüft möglicherweise Links

Erweiterte Problemlösung

Logging aktivieren (für Support)

Die Anwendung schreibt Debug-Informationen in die Ausgabe. Bei Problemen:

1. Programm aus Kommandozeile starten
2. Fehler-Output dokumentieren
3. An Support senden

Neuinstallation

Bei persistenten Problemen:

1. Programm-Ordner vollständig löschen
2. Neue Version herunterladen
3. An neuem Speicherort entpacken
4. Erneut testen

Systemvoraussetzungen prüfen

Stellen Sie sicher:

- Windows 10 oder neuer
- .NET Framework 4.7.2+ oder .NET 5+
- Mindestens 4 GB RAM
- Aktive Internetverbindung

Support kontaktieren

Bei ungelösten Problemen:

Benötigte Informationen:

- Windows-Version
- .NET-Version
- Fehlermeldung (Screenshot)
- Schritte zur Reproduktion
- Anzahl geladener Einträge

Kontakt:

- Webseite: https://www.it-service-walter.com
- Beschreiben Sie das Problem detailliert
- Fügen Sie Screenshots bei

Anhang A: Tastenkombinationen

Tastenkombination	Funktion
F5	Daten neu laden
Strg + F	Fokus auf Suchfeld
Strg + R	Filter zurücksetzen
Strg + E	Excel-Export
Strg + H	Hilfe öffnen
Esc	Dialog schließen

Hinweis: Nicht alle Tastenkombinationen sind in der aktuellen Version implementiert.

Anhang B: Glossar

Advisory: Sicherheitsmeldung, die vor Schwachstellen warnt und Lösungen bereitstellt.

API: Application Programming Interface - Schnittstelle zum Datenaustausch.

CERT: Computer Emergency Response Team - Organisation für IT-Sicherheit.

CVSS: Common Vulnerability Scoring System - Standard zur Bewertung von Sicherheitslücken.

CVE: Common Vulnerabilities and Exposures - Eindeutige Kennung für Sicherheitslücken.

Mitigation: Maßnahmen zur Schadensbegrenzung (z.B. Patches, Workarounds).

Patch: Software-Update zur Behebung von Sicherheitslücken.

Severity: Schweregrad einer Sicherheitslücke.

Vulnerability: Sicherheitslücke oder Schwachstelle in Software/Hardware.

Workaround: Behelfslösung wenn kein Patch verfügbar ist.

Dokumentversion: 1.0
Stand: Januar 2025
Entwickelt von: IT-Service Walter
Kontakt: https://www.it-service-walter.com

Für weitere Unterstützung kontaktieren Sie bitte:
IT-Service Walter
Jörn Walter
Mittelstr. 65, 53879 Euskirchen
Web: https://www.it-service-walter.com
E-Mail: info@it-service-walter.com

📜 Rechtliche Hinweise

Verkauf

Die Software kostet für den Einzelplatz 59,00 € inkl. 19% MwSt. Als Firmenlizenz einmalig 249,00 € inkl. 19% MwSt.