

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240806



## Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>1 Editorial</b>   | <b>2</b>  |
| <b>2 Security-News</b>   | <b>3</b>  |
| 2.1 Heise - Security-Alert . . . . .   | 3         |
| <b>3 Sicherheitslücken</b>   | <b>4</b>  |
| 3.1 EPSS . . . . .   | 4         |
| 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .                                | 5         |
| 3.2 BSI - Warn- und Informationsdienst (WID) . . . . .                                   | 7         |
| 3.3 Sicherheitslücken Meldungen von Tenable . . . . .                                    | 11        |
| <b>4 Aktiv ausgenutzte Sicherheitslücken</b>   | <b>13</b> |
| 4.1 Exploits der letzten 5 Tage . . . . .  | 13        |
| 4.2 0-Days der letzten 5 Tage . . . . .  | 16        |
| <b>5 Die Hacks der Woche</b>   | <b>22</b> |
| 5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . . | 22        |
| <b>6 Cyberangriffe: (Aug)</b>  | <b>23</b> |
| <b>7 Ransomware-Erpressungen: (Aug)</b>  | <b>23</b> |
| <b>8 Quellen</b>   | <b>25</b> |
| 8.1 Quellenverzeichnis . . . . .   | 25        |
| <b>9 Impressum</b>   | <b>26</b> |

## 1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

#### ***Kritische Sicherheitslücke bedroht Unternehmenssoftware Apache OFBiz***

Angreifer können Systeme mit Apache OFBiz attackieren und eigenen Code ausführen. Eine dagegen abgesicherte Version steht zum Download bereit.

- [Link](#)

—

#### ***Unbefugte Zugriffe auf IT-Managementlösung Aruba ClearPass möglich***

Die Entwickler von HPE Aruba Networking haben in ClearPass Policy Manager unter anderem eine kritische Sicherheitslücke geschlossen.

- [Link](#)

—

#### ***Kritische Sicherheitslücke bedroht Google Chrome***

Angreifer können an mehreren Schwachstellen in Chrome ansetzen, um PCs zu kompromittieren.

- [Link](#)

—

#### ***Keine Sicherheitsupdates in Sicht: Avast Free Antivirus ist verwundbar***

Sicherheitsforscher warnen vor Schwachstellen in Avast Free Antivirus und raten aufgrund fehlender Patches von einer Nutzung ab.

- [Link](#)

—

#### ***Jetzt patchen! Ransomware-Attacken auf VMware ESXi-Server beobachtet***

Sicherheitsforscher warnen vor laufenden Attacken auf Systeme mit ESXi-Hypervisor. Darüber gelangen Erpressungstrojaner auf Computer.

- [Link](#)

—

#### ***Selenium Grid: Unsichere Standardkonfiguration lässt Krypto-Miner passieren***

Das Framework für automatisierte Softwaretests Selenium Grid ist in den Standardeinstellungen verwundbar. Das nutzen Angreifer derzeit aus.

- [Link](#)

—

#### ***Angreifer nutzen Schadcode-Lücke in Acronis Cyber Infrastructure aus***

In mehreren aktualisierten Versionen von Acronis Cyber Infrastructure haben die Entwickler eine kritische Lücke geschlossen.

- [Link](#)

—

***Sicherheitsupdate schützt SolarWinds Platform vor möglichen Attacken***

Angreifer können die IT-Verwaltungssoftware SolarWinds Platform attackieren. Die Entwickler haben mehrere Schwachstellen geschlossen.

- [Link](#)

—

***Sicherheitslücke: Entwickler raten zum zügigen Patchen von Telerik Report Server***

Ein wichtiges Sicherheitsupdate schließt eine kritische Lücke in der IT-Management- und Reporting-Lösung Telerik Report Server.

- [Link](#)

—

***Jetzt patchen! Angreifer attackieren Now Platform von ServiceNow***

Die Cloud Computing Plattform von ServiceNow ist derzeit im Visier von Angreifern und sie nutzen kritische Sicherheitslücken aus.

- [Link](#)

—

### 3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

#### 3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

| CVE            | EPSS        | Perzentil   | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-7028  | 0.903160000 | 0.988520000 | <a href="#">Link</a>  |
| CVE-2023-6895  | 0.922010000 | 0.989880000 | <a href="#">Link</a>  |
| CVE-2023-6553  | 0.925190000 | 0.990280000 | <a href="#">Link</a>  |
| CVE-2023-5360  | 0.903980000 | 0.988580000 | <a href="#">Link</a>  |
| CVE-2023-52251 | 0.940460000 | 0.991890000 | <a href="#">Link</a>  |
| CVE-2023-4966  | 0.971280000 | 0.998250000 | <a href="#">Link</a>  |
| CVE-2023-49103 | 0.962110000 | 0.995470000 | <a href="#">Link</a>  |
| CVE-2023-48795 | 0.964660000 | 0.996100000 | <a href="#">Link</a>  |
| CVE-2023-47246 | 0.957550000 | 0.994650000 | <a href="#">Link</a>  |
| CVE-2023-46805 | 0.936080000 | 0.991380000 | <a href="#">Link</a>  |
| CVE-2023-46747 | 0.972730000 | 0.998790000 | <a href="#">Link</a>  |
| CVE-2023-46604 | 0.961790000 | 0.995420000 | <a href="#">Link</a>  |
| CVE-2023-4542  | 0.928310000 | 0.990560000 | <a href="#">Link</a>  |
| CVE-2023-43208 | 0.965360000 | 0.996360000 | <a href="#">Link</a>  |
| CVE-2023-43177 | 0.965600000 | 0.996440000 | <a href="#">Link</a>  |
| CVE-2023-42793 | 0.970370000 | 0.997870000 | <a href="#">Link</a>  |
| CVE-2023-41265 | 0.911110000 | 0.989070000 | <a href="#">Link</a>  |
| CVE-2023-39143 | 0.941900000 | 0.992090000 | <a href="#">Link</a>  |
| CVE-2023-38646 | 0.906610000 | 0.988760000 | <a href="#">Link</a>  |
| CVE-2023-38205 | 0.947910000 | 0.992980000 | <a href="#">Link</a>  |
| CVE-2023-38203 | 0.966410000 | 0.996630000 | <a href="#">Link</a>  |
| CVE-2023-38035 | 0.974680000 | 0.999710000 | <a href="#">Link</a>  |
| CVE-2023-36845 | 0.964250000 | 0.996010000 | <a href="#">Link</a>  |

| CVE            | EPSS        | Perzentil   | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-3519  | 0.965340000 | 0.996350000 | <a href="#">Link</a>  |
| CVE-2023-35082 | 0.968030000 | 0.997130000 | <a href="#">Link</a>  |
| CVE-2023-35078 | 0.970390000 | 0.997880000 | <a href="#">Link</a>  |
| CVE-2023-34993 | 0.972640000 | 0.998760000 | <a href="#">Link</a>  |
| CVE-2023-34960 | 0.936550000 | 0.991440000 | <a href="#">Link</a>  |
| CVE-2023-34634 | 0.930910000 | 0.990870000 | <a href="#">Link</a>  |
| CVE-2023-34468 | 0.906650000 | 0.988760000 | <a href="#">Link</a>  |
| CVE-2023-34362 | 0.969450000 | 0.997550000 | <a href="#">Link</a>  |
| CVE-2023-34039 | 0.944910000 | 0.992550000 | <a href="#">Link</a>  |
| CVE-2023-3368  | 0.935570000 | 0.991320000 | <a href="#">Link</a>  |
| CVE-2023-33246 | 0.972140000 | 0.998550000 | <a href="#">Link</a>  |
| CVE-2023-32315 | 0.970550000 | 0.997950000 | <a href="#">Link</a>  |
| CVE-2023-30625 | 0.948260000 | 0.993050000 | <a href="#">Link</a>  |
| CVE-2023-30013 | 0.962790000 | 0.995630000 | <a href="#">Link</a>  |
| CVE-2023-29300 | 0.968930000 | 0.997360000 | <a href="#">Link</a>  |
| CVE-2023-29298 | 0.943640000 | 0.992340000 | <a href="#">Link</a>  |
| CVE-2023-28432 | 0.906190000 | 0.988710000 | <a href="#">Link</a>  |
| CVE-2023-28343 | 0.923780000 | 0.990100000 | <a href="#">Link</a>  |
| CVE-2023-28121 | 0.909500000 | 0.988940000 | <a href="#">Link</a>  |
| CVE-2023-27524 | 0.970600000 | 0.997970000 | <a href="#">Link</a>  |
| CVE-2023-27372 | 0.973190000 | 0.998990000 | <a href="#">Link</a>  |
| CVE-2023-27350 | 0.969960000 | 0.997730000 | <a href="#">Link</a>  |
| CVE-2023-26469 | 0.956500000 | 0.994490000 | <a href="#">Link</a>  |
| CVE-2023-26360 | 0.959350000 | 0.994950000 | <a href="#">Link</a>  |
| CVE-2023-26035 | 0.967950000 | 0.997100000 | <a href="#">Link</a>  |
| CVE-2023-25717 | 0.954090000 | 0.994010000 | <a href="#">Link</a>  |
| CVE-2023-25194 | 0.968820000 | 0.997350000 | <a href="#">Link</a>  |

| CVE            | EPSS        | Perzentil   | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-2479  | 0.963740000 | 0.995870000 | <a href="#">Link</a>  |
| CVE-2023-24489 | 0.973540000 | 0.999130000 | <a href="#">Link</a>  |
| CVE-2023-23752 | 0.956380000 | 0.994470000 | <a href="#">Link</a>  |
| CVE-2023-23333 | 0.958950000 | 0.994870000 | <a href="#">Link</a>  |
| CVE-2023-22527 | 0.968290000 | 0.997180000 | <a href="#">Link</a>  |
| CVE-2023-22518 | 0.964890000 | 0.996150000 | <a href="#">Link</a>  |
| CVE-2023-22515 | 0.973730000 | 0.999210000 | <a href="#">Link</a>  |
| CVE-2023-21839 | 0.957210000 | 0.994580000 | <a href="#">Link</a>  |
| CVE-2023-21554 | 0.952830000 | 0.993760000 | <a href="#">Link</a>  |
| CVE-2023-20887 | 0.970670000 | 0.997990000 | <a href="#">Link</a>  |
| CVE-2023-1698  | 0.910560000 | 0.989030000 | <a href="#">Link</a>  |
| CVE-2023-1671  | 0.962480000 | 0.995550000 | <a href="#">Link</a>  |
| CVE-2023-0669  | 0.969440000 | 0.997530000 | <a href="#">Link</a>  |

### 3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 05 Aug 2024

#### **[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Mon, 05 Aug 2024

#### **[NEU] [UNGEPATCHT] [hoch] Checkmk: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle in Checkmk ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—



Mon, 05 Aug 2024

**[NEU] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 05 Aug 2024

**[NEU] [hoch] Apache OFBiz: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache OFBiz ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 05 Aug 2024

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Mon, 05 Aug 2024

**[UPDATE] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in docker ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 02 Aug 2024

**[NEU] [hoch] Microsoft Dynamics 365: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft Dynamics 365 ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 02 Aug 2024

**[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um Informationen offenzulegen oder beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 02 Aug 2024

***[UPDATE] [hoch] Apache Tomcat: Schwachstelle ermöglicht Privilegieneskalation***

Ein lokaler Angreifer kann eine Schwachstelle in Apache Tomcat ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 02 Aug 2024

***[UPDATE] [kritisch] Apache Tomcat: Schwachstelle ermöglicht Denial of Service***

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Apache Tomcat ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 02 Aug 2024

***[UPDATE] [hoch] IBM MQ: Mehrere Schwachstellen***

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in IBM MQ ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 02 Aug 2024

***[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung***

Ein entfernter, anonym Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- [Link](#)

—

Fri, 02 Aug 2024

***[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen***

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen oder einen unspezifischen Angriff durchzuführen.

- [Link](#)

—

Fri, 02 Aug 2024

***[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff***

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 02 Aug 2024

**[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- [Link](#)

—

Fri, 02 Aug 2024

**[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- [Link](#)

—

Fri, 02 Aug 2024

**[NEU] [hoch] Rockwell Automation ControlLogix: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Rockwell Automation ControlLogix ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 01 Aug 2024

**[UPDATE] [hoch] expat: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in expat ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 01 Aug 2024

**[UPDATE] [hoch] libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff**

Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Thu, 01 Aug 2024

**[UPDATE] [hoch] Broadcom Brocade Switch: Mehrere Schwachstellen**

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Broadcom Brocade Switch und Broadcom Fabric OS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen und vertrauliche Informationen preiszugeben.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

| Datum    | Schwachstelle   | Bewertung |
|----------|---|-----------|
| 8/5/2024 | [Fedora 40 : trafficserver (2024-77fe791124)]   | critical  |
| 8/5/2024 | [Fedora 39 : trafficserver (2024-2243c5abee)]   | critical  |
| 8/3/2024 | [SUSE SLES12 Security Update : docker (SUSE-SU-2024:2709-1)]  | critical  |
| 8/2/2024 | [OSGeo GeoTools RCE (CVE-2024-36404)]   | critical  |
| 8/2/2024 | [OSGeo GeoServer RCE (CVE-2024-36401)]  | critical  |
| 8/1/2024 | [Fedora 40 : kernel (2024-873e2cb5f2)]  | critical  |
| 8/1/2024 | [Amazon Linux 2 : docker (ALASDOCKER-2024-040)]   | critical  |
| 8/1/2024 | [RHEL 8 : emacs (RHSA-2024:4971)]   | critical  |
| 8/1/2024 | [Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Gross vulnerability (USN-6942-1)] | critical  |
| 8/1/2024 | [Amazon Linux 2023 : docker (ALAS2023-2024-674)]  | critical  |
| 8/5/2024 | [Fedora 39 : ffmpeg (2024-4d2c8e6f85)]  | high      |
| 8/5/2024 | [Debian dsa-5736 : openjdk-11-dbg - security update]  | high      |
| 8/5/2024 | [Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1)]                          | high      |
| 8/5/2024 | [Debian dsa-5737 : fonts-opensymbol - security update]  | high      |
| 8/3/2024 | [Photon OS 3.0: Runc PHSA-2024-3.0-0775]  | high      |
| 8/3/2024 | [Fedora 39 : chromium (2024-ff743391c3)]  | high      |
| 8/3/2024 | [SUSE SLES15 Security Update : kernel RT (Live Patch 8 for SLE 15 SP5) (SUSE-SU-2024:2719-1)]         | high      |
| 8/3/2024 | [SUSE SLES15 Security Update : kernel RT (Live Patch 10 for SLE 15 SP5) (SUSE-SU-2024:2722-1)]        | high      |
| 8/3/2024 | [SUSE SLES15 Security Update : kernel RT (Live Patch 15 for SLE 15 SP5) (SUSE-SU-2024:2723-1)]        | high      |

| Datum    | Schwachstelle   | Bewertung |
|----------|---|-----------|
| 8/3/2024 | [Fedora 40 : chromium (2024-3a1a0a664e)]  | high      |
| 8/3/2024 | [Fedora 40 : bind / bind-dyndb-ldap (2024-8af1780fdf)]  | high      |
| 8/3/2024 | [Fedora 40 : hostapd / wpa_supplicant (2024-73626281d8)]  | high      |
| 8/2/2024 | [Photon OS 5.0: Python3 PHSA-2024-5.0-0338]   | high      |
| 8/2/2024 | [ImageMagick < 7.11-36 Arbitrary Code Execution]  | high      |
| 8/2/2024 | [Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-6895-4)]                                      | high      |
| 8/2/2024 | [WordPress < 6.6.1]   | high      |
| 8/2/2024 | [Progress MOVEit Transfer < 2023.0.12 / 2023.1 < 2023.1.7 / 2024.0 < 2024.0.3 Privilege Escalation] | high      |
| 8/2/2024 | [ManageEngine OpManager SQLi (CVE-2024-6748)]   | high      |
| 8/1/2024 | [Slackware Linux 15.0 / current curl Vulnerability (SSA:2024-213-01)]                               | high      |
| 8/1/2024 | [FreeBSD : chromium – multiple security fixes (15d398ea-4f73-11ef-8a0f-a8a1599412c6)]               | high      |
| 8/1/2024 | [RHEL 8 : kpatch-patch-4_18_0-305_120_1 (RHSA-2024:4970)]   | high      |
| 8/1/2024 | [Ubuntu 14.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-6926-2)]                          | high      |
| 8/1/2024 | [Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.5.6.5)]   | high      |
| 8/1/2024 | [Microsoft Edge (Chromium) < 127.0.2651.86 Multiple Vulnerabilities]                                | high      |
| 8/1/2024 | [Ubuntu 18.04 LTS : Bind vulnerabilities (USN-6909-2)]  | high      |
| 8/1/2024 | [Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Tomcat vulnerabilities (USN-6943-1)]        | high      |

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Mon, 05 Aug 2024

**Linux DRM `drm_file_update_pid()` Race Condition / Use-After-Free**

Linux DRM has `drm_file_update_pid()` call to `get_pid()` too late, which creates a race condition that can lead to use-after-free issue of a struct pid.

- [Link](#)

—

” “Mon, 05 Aug 2024

**Online Shopping Portal Project 2.0 SQL Injection**

Online Shopping Portal Project version 2.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

**Dolphin 7.4.2 Blind SQL Injection**

Dolphin version 7.4.2 suffers from a remote blind SQL injection vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

**Ivanti ADC 9.9 Authentication Bypass**

Ivanti ADC version 9.9 suffers from an authentication bypass vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

**Genexus Protection Server 9.7.2.10 Unquoted Service Path**

Genexus Protection Server version 9.7.2.10 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

**Devika 1 Path Traversal**

Devika version 1 suffers from a path traversal vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

**e107 2.3.3 Cross Site Scripting**

e107 version 2.3.3 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

***Codeprojects E-Commerce 1.0 Insecure Settings***

Codeprojects E-Commerce version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Mon, 05 Aug 2024

***Blog Site 1.0 SQL Injection***

Blog Site version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 05 Aug 2024

***Best Courier Management System 1.0 SQL Injection***

Best Courier Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 05 Aug 2024

***Appointment Scheduler 4.0 Insecure Direct Object Reference***

Appointment Scheduler version 4.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Fri, 02 Aug 2024

***Packet Storm New Exploits For July, 2024***

This archive contains all of the 105 exploits added to Packet Storm in July, 2024.

- [Link](#)

—

” “Fri, 02 Aug 2024

***Tourism Management System 2.0 Cross Site Scripting***

Tourism Management System version 2.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 02 Aug 2024

***Computer Laboratory Management System 1.0 Privilege Escalation***

Computer Laboratory Management System version 1.0 suffers from an incorrect access control that allows for privilege escalation.

- [Link](#)

—

” “Fri, 02 Aug 2024

***Leads Manager Tool SQL Injection / Cross Site Scripting***

Leads Manager Tool suffers from remote SQL injection and cross site scripting vulnerabilities.

- [Link](#)

—

” “Fri, 02 Aug 2024

***ReadyMade Unilevel Ecommerce MLM Blind SQL Injection / Cross Site Scripting***

Readymade Unilevel Ecommerce MLM suffers from remote blind SQL injection and cross site scripting vulnerabilities. These issues affected the version released as late as March 15, 2024.

- [Link](#)

—

” “Fri, 02 Aug 2024

***Appointment Scheduler 3.0 Insecure Direct Object Reference***

Appointment Scheduler version 3.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Fri, 02 Aug 2024

***AccPack Cop 1.0 Cross Site Request Forgery***

AccPack Cop version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Fri, 02 Aug 2024

***AccPack Buzz 1.0 SQL Injection***

AccPack Buzz version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Thu, 01 Aug 2024

***Availability Calendar 5.0 Insecure Direct Object Reference***

Availability Calendar version 5.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Thu, 01 Aug 2024

***Oracle Database 12c Release 1 Unquoted Service Path***

Oracle Database version 12c Release 1 suffers from an unquoted service path vulnerability.

- [Link](#)



—

” “Thu, 01 Aug 2024

***SolarWinds Kiwi Syslog Server 9.6.7.1 Unquoted Service Path***

SolarWinds Kiwi Syslog Server version 9.6.7.1 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Thu, 01 Aug 2024

***Babaji E-Commerce 1.0 Insecure Settings***

Babaji E-Commerce version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Wed, 31 Jul 2024

***OpenMediaVault rpc.php Authenticated Cron Remote Code Execution***

OpenMediaVault allows an authenticated user to create cron jobs as root on the system. An attacker can abuse this by sending a POST request via rpc.php to schedule and execute a cron entry that runs arbitrary commands as root on the system. All OpenMediaVault versions including the latest release 7.4.2-2 are vulnerable.

- [Link](#)

—

” “Wed, 31 Jul 2024

***Readymade Real Estate Script SQL Injection / Cross Site Scripting***

Readymade Real Estate Script suffers from remote blind SQL injection and cross site scripting vulnerabilities. This was last validated on the build available as of July 12, 2024.

- [Link](#)

—

”

## **4.2 0-Days der letzten 5 Tage**

“Mon, 05 Aug 2024

***ZDI-24-1087: (0Day) oFono SMS Decoder Stack-based Buffer Overflow Privilege Escalation Vulnerability***

- [Link](#)

—

” “Mon, 05 Aug 2024

***ZDI-24-1086: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability***

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1085: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1084: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1083: (0Day) oFono SimToolKit Heap-based Buffer Overflow Privilege Escalation Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1082: (0Day) (Pwn2Own) oFono AT CMGR Command Uninitialized Variable Information Disclosure Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1081: (0Day) (Pwn2Own) oFono AT CMT Command Uninitialized Variable Information Disclosure Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1080: (0Day) (Pwn2Own) oFono AT CMGL Command Uninitialized Variable Information Disclosure Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1079: (0Day) (Pwn2Own) oFono CUSD Stack-based Buffer Overflow Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1078: (0Day) (Pwn2Own) oFono CUSD AT Command Stack-based Buffer Overflow Code**

—

**Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1077: (0Day) (Pwn2Own) oFono QMI SMS Handling Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1076: Microsoft Windows Menu DC Color Space Use-After-Free Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1075: Microsoft PowerShell Reference for Office Products officedocs-cdn Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1074: Microsoft PowerShell Gallery psg-prod-centralus Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1073: Microsoft Azure uAMQP azure-iot-sdks-ci Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1072: Microsoft CameraTraps cameratracsppftkje Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1071: Microsoft Azure GPT ALE palantirdemoacr Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1070: Microsoft Partner Resources openhacks Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1069: Microsoft Technical Case Studies athena-dashboard Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1068: Microsoft Azure ML.NET Samples mlnetfilestorage Uncontrolled Search Path Element Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1067: Microsoft Azure CollectSFData docs-analytics-eus Uncontrolled Search Path Element Impersonation Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1066: Microsoft Azure DataStoriesSamples machinelearningdatasets Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1065: Microsoft Azure Availability Monitor for Kafka esnewdeveastdockerregistry Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1064: Microsoft AirSim airsimci Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1063: Microsoft Reactor Workshops reactorworkshops Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1062: Microsoft Fluid Framework prague Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1061: Microsoft What The Hack docsmsftpdfs Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1060: Microsoft Azure Aztask aztask1528763526 Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1059: Microsoft Azure Linux Automation konkaciwestus1 Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1058: Microsoft Azure NodeJS LogPoint logpointsassets Uncontrolled Search Path Element Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1057: Trimble SketchUp Pro SKP File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

**ZDI-24-1056: Trimble SketchUp SKP File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 05 Aug 2024

***ZDI-24-1055: Trimble SketchUp SKP File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 05 Aug 2024

***ZDI-24-1054: Trimble SketchUp Viewer SKP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Aug)

| Datum      | Opfer | Land  | Information          |
|------------|-------|-------|----------------------|
| 2024-08-03 | Xtrim | [ECU] | <a href="#">Link</a> |

## 7 Ransomware-Erpressungen: (Aug)

| Datum      | Opfer                            | Ransomware-Gruppe | Webseite             |
|------------|----------------------------------|-------------------|----------------------|
| 2024-08-05 | [Silipos]                        | cicada3301        | <a href="#">Link</a> |
| 2024-08-04 | [kierlcpa.com]                   | lockbit3          | <a href="#">Link</a> |
| 2024-08-05 | [Square One Coating Systems]     | cicada3301        | <a href="#">Link</a> |
| 2024-08-05 | [Hi-P International]             | fog               | <a href="#">Link</a> |
| 2024-08-05 | [Zon Beachside zonbeachside.com] | dispossessor      | <a href="#">Link</a> |
| 2024-08-05 | [HP Distribution]                | incransom         | <a href="#">Link</a> |
| 2024-08-05 | [exco-solutions.com]             | cactus            | <a href="#">Link</a> |
| 2024-08-05 | [Maryville Academy]              | rhysida           | <a href="#">Link</a> |
| 2024-08-04 | [notariusze.waw.pl]              | killsec           | <a href="#">Link</a> |
| 2024-08-04 | [Ranney School]                  | rhysida           | <a href="#">Link</a> |
| 2024-08-03 | [nursing.com]                    | ransomexx         | <a href="#">Link</a> |
| 2024-08-03 | [Bettis Asphalt]                 | blacksuit         | <a href="#">Link</a> |
| 2024-08-03 | [fcl.crs]                        | lockbit3          | <a href="#">Link</a> |
| 2024-08-03 | [CPA Tax Solutions]              | meow              | <a href="#">Link</a> |
| 2024-08-03 | [LRN]                            | hunters           | <a href="#">Link</a> |
| 2024-08-03 | [aikenhousing.org]               | blacksuit         | <a href="#">Link</a> |
| 2024-08-02 | [David E Shambach Architect]     | dragonforce       | <a href="#">Link</a> |
| 2024-08-02 | [Hayes Beer Distributing]        | dragonforce       | <a href="#">Link</a> |
| 2024-08-02 | [Jangho Group]                   | hunters           | <a href="#">Link</a> |



| Datum      | Opfer                                  | Ransomware-Gruppe | Webseite             |
|------------|--|-------------------|----------------------|
| 2024-08-02 | [Khandelwal Laboratories Pvt]          | hunters           | <a href="#">Link</a> |
| 2024-08-02 | [retaildatallc.com]                    | ransomhub         | <a href="#">Link</a> |
| 2024-08-02 | [WPG Holdings]                         | meow              | <a href="#">Link</a> |
| 2024-08-02 | [National Beverage]                    | meow              | <a href="#">Link</a> |
| 2024-08-02 | [PeoplesHR]                            | meow              | <a href="#">Link</a> |
| 2024-08-02 | [Dometic Group]                        | meow              | <a href="#">Link</a> |
| 2024-08-02 | [Remitano]                             | meow              | <a href="#">Link</a> |
| 2024-08-02 | [Premier Equities]                     | meow              | <a href="#">Link</a> |
| 2024-08-01 | [Kemlon Products & Development Co Inc] | spacebears        | <a href="#">Link</a> |
| 2024-08-02 | [q-cells.de]                           | abyss             | <a href="#">Link</a> |
| 2024-08-02 | [coinbv.nl]                            | madliberator      | <a href="#">Link</a> |
| 2024-08-01 | [Valley Bulk]                          | cicada3301        | <a href="#">Link</a> |
| 2024-08-01 | [ENEA Italy]                           | hunters           | <a href="#">Link</a> |
| 2024-08-01 | [mcdowallaffleck.com.au]               | ransomhub         | <a href="#">Link</a> |
| 2024-08-01 | [effinghamschools.com]                 | ransomhub         | <a href="#">Link</a> |
| 2024-08-01 | [warrendale-wagyu.co.uk]               | darkvault         | <a href="#">Link</a> |
| 2024-08-01 | [Adorna & Guzman Dentistry]            | monti             | <a href="#">Link</a> |
| 2024-08-01 | [Camp Susque]                          | medusa            | <a href="#">Link</a> |
| 2024-08-01 | [Ali Gohar]                            | medusa            | <a href="#">Link</a> |
| 2024-08-01 | [acsi.org]                             | blacksuit         | <a href="#">Link</a> |
| 2024-08-01 | [County Linen UK]                      | dispossessor      | <a href="#">Link</a> |
| 2024-08-01 | [TNT Materials tnt-materials.com/]     | dispossessor      | <a href="#">Link</a> |
| 2024-08-01 | [Peñoles]                              | akira             | <a href="#">Link</a> |
| 2024-08-01 | [dahlvalve.com]                        | cactus            | <a href="#">Link</a> |

## 8 Quellen

### 8.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - [packetstormsecurity.com](https://packetstormsecurity.com)
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

## 9 Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

[info@cyberwald.com](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.