

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240728



## 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 . . . . .	17
<b>5 Die Hacks der Woche</b>	<b>20</b>
5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . .	20
<b>6 Cyberangriffe: (Jul)</b>	<b>21</b>
<b>7 Ransomware-Erpressungen: (Jul)</b>	<b>22</b>
<b>8 Quellen</b>	<b>36</b>
8.1 Quellenverzeichnis . . . . .	36
<b>9 Impressum</b>	<b>37</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

***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](#)

—

***Sicherheitsupdates: Aruba EdgeConnect SD-WAN vielfältig attackierbar***

Die Entwickler von HPE haben in Arubas SD-WAN-Lösung EdgeConnect mehrere gefährliche Sicherheitslücken geschlossen.

- [Link](#)

—

***Docker: Alte Sicherheitslücke zur Rechteausweitung wieder aufgetaucht***

Eine Schwachstelle in den Autorisierung-Plug-ins hatte Docker 2019 geschlossen. Sie ist aber kurz danach als Regression wieder in die Engine eingeflossen.

- [Link](#)

—

***Siemens SICAM: Angreifer können Admin-Passwort zurücksetzen***

SCADA-Systeme der SICAM-Reihe von Siemens kommen in kritischen Infrastrukturen zum Einsatz. Sicherheitsupdates schließen eine kritische Lücke.

- [Link](#)

—

***Software-Distributionssystem TeamCity erinnert sich an gelöschte Zugangstoken***

Angreifer können an sechs mittlerweile geschlossenen Sicherheitslücken in JetBrains TeamCity ansetzen.

- [Link](#)

—

***Backup-System Data Protection Advisor von Dell vielfältig angreifbar***

Dell hat mehrere Sicherheitslücken in Data Protection Advisor geschlossen. Es kann Schadcode auf Systeme gelangen.

- [Link](#)

---

**BIOS-Sicherheitslücke gefährdet unzählige HP-PCs**

Angreifer können viele Desktopcomputer von HP mit Schadcode attackieren.

- [Link](#)

---

**Sicherheitsupdates: Angreifer können Sonicwall-Firewalls lahmlegen**

Einige Firewalls von Sonicwall sind verwundbar. Attacken könnten bevorstehen.

- [Link](#)

---

**SolarWinds Access Rights Manager: Angreifer mit Systemrechten und Schadcode**

Die Entwickler haben in SolarWinds ARM acht kritische Sicherheitslücken geschlossen.

- [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	0.988570000	<a href="#">Link</a>
CVE-2023-6895	0.922010000	0.989960000	<a href="#">Link</a>
CVE-2023-6553	0.937510000	0.991600000	<a href="#">Link</a>
CVE-2023-5360	0.903980000	0.988640000	<a href="#">Link</a>
CVE-2023-52251	0.938200000	0.991690000	<a href="#">Link</a>
CVE-2023-4966	0.971710000	0.998370000	<a href="#">Link</a>
CVE-2023-49103	0.953130000	0.993890000	<a href="#">Link</a>
CVE-2023-48795	0.964660000	0.996120000	<a href="#">Link</a>
CVE-2023-47246	0.948140000	0.993060000	<a href="#">Link</a>
CVE-2023-46805	0.936080000	0.991430000	<a href="#">Link</a>
CVE-2023-46747	0.972730000	0.998750000	<a href="#">Link</a>
CVE-2023-46604	0.963510000	0.995860000	<a href="#">Link</a>
CVE-2023-4542	0.928310000	0.990610000	<a href="#">Link</a>
CVE-2023-43208	0.964870000	0.996180000	<a href="#">Link</a>
CVE-2023-43177	0.962660000	0.995640000	<a href="#">Link</a>
CVE-2023-42793	0.970370000	0.997900000	<a href="#">Link</a>
CVE-2023-41265	0.905890000	0.988760000	<a href="#">Link</a>
CVE-2023-39143	0.938190000	0.991680000	<a href="#">Link</a>
CVE-2023-38646	0.906610000	0.988840000	<a href="#">Link</a>
CVE-2023-38205	0.954590000	0.994170000	<a href="#">Link</a>
CVE-2023-38203	0.966410000	0.996640000	<a href="#">Link</a>
CVE-2023-38146	0.915710000	0.989420000	<a href="#">Link</a>
CVE-2023-38035	0.974400000	0.999580000	<a href="#">Link</a>
CVE-2023-36845	0.961840000	0.995480000	<a href="#">Link</a>
CVE-2023-3519	0.965340000	0.996380000	<a href="#">Link</a>
CVE-2023-35082	0.968030000	0.997160000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968330000	0.997250000	<a href="#">Link</a>
CVE-2023-34993	0.972880000	0.998840000	<a href="#">Link</a>
CVE-2023-34960	0.936550000	0.991500000	<a href="#">Link</a>
CVE-2023-34634	0.930910000	0.990910000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988840000	<a href="#">Link</a>
CVE-2023-34362	0.969450000	0.997570000	<a href="#">Link</a>
CVE-2023-34039	0.940490000	0.991940000	<a href="#">Link</a>
CVE-2023-3368	0.935570000	0.991370000	<a href="#">Link</a>
CVE-2023-33246	0.972610000	0.998710000	<a href="#">Link</a>
CVE-2023-32315	0.973620000	0.999160000	<a href="#">Link</a>
CVE-2023-30625	0.948260000	0.993090000	<a href="#">Link</a>
CVE-2023-30013	0.962790000	0.995690000	<a href="#">Link</a>
CVE-2023-29300	0.968930000	0.997410000	<a href="#">Link</a>
CVE-2023-29298	0.943640000	0.992380000	<a href="#">Link</a>
CVE-2023-28771	0.902140000	0.988510000	<a href="#">Link</a>
CVE-2023-28343	0.949510000	0.993260000	<a href="#">Link</a>
CVE-2023-28121	0.909760000	0.989020000	<a href="#">Link</a>
CVE-2023-27524	0.970300000	0.997880000	<a href="#">Link</a>
CVE-2023-27372	0.972890000	0.998850000	<a href="#">Link</a>
CVE-2023-27350	0.969960000	0.997760000	<a href="#">Link</a>
CVE-2023-26469	0.951490000	0.993570000	<a href="#">Link</a>
CVE-2023-26360	0.959350000	0.995000000	<a href="#">Link</a>
CVE-2023-26035	0.967950000	0.997140000	<a href="#">Link</a>
CVE-2023-25717	0.954090000	0.994050000	<a href="#">Link</a>
CVE-2023-25194	0.968820000	0.997400000	<a href="#">Link</a>
CVE-2023-2479	0.963740000	0.995920000	<a href="#">Link</a>
CVE-2023-24489	0.973720000	0.999200000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.954250000	0.994110000	<a href="#">Link</a>
CVE-2023-23397	0.901800000	0.988490000	<a href="#">Link</a>
CVE-2023-23333	0.959750000	0.995070000	<a href="#">Link</a>
CVE-2023-22527	0.970550000	0.997970000	<a href="#">Link</a>
CVE-2023-22518	0.964890000	0.996190000	<a href="#">Link</a>
CVE-2023-22515	0.973590000	0.999160000	<a href="#">Link</a>
CVE-2023-21839	0.957210000	0.994610000	<a href="#">Link</a>
CVE-2023-21554	0.952830000	0.993820000	<a href="#">Link</a>
CVE-2023-20887	0.970170000	0.997820000	<a href="#">Link</a>
CVE-2023-1698	0.910560000	0.989090000	<a href="#">Link</a>
CVE-2023-1671	0.962480000	0.995600000	<a href="#">Link</a>
CVE-2023-0669	0.969440000	0.997560000	<a href="#">Link</a>

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

Fri, 26 Jul 2024

**[NEU] [hoch] Progress Software Telerik Report Server: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Progress Software Telerik Report Server ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 26 Jul 2024

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

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

- [Link](#)

—

Fri, 26 Jul 2024

**[NEU] [hoch] Apache Traffic Server: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Traffic Server ausnutzen,



um einen Denial of Service Angriff durchzuführen oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Fri, 26 Jul 2024

**[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection**

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- [Link](#)

—

Fri, 26 Jul 2024

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

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

- [Link](#)

—

Fri, 26 Jul 2024

**[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- [Link](#)

—

Fri, 26 Jul 2024

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

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

- [Link](#)

—

Fri, 26 Jul 2024

**[UPDATE] [hoch] Microsoft Windows: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 26 Jul 2024

**[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen**

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- [Link](#)

—

Fri, 26 Jul 2024

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

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

- [Link](#)

—

Fri, 26 Jul 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](#)

—

Fri, 26 Jul 2024

**[UPDATE] [hoch] Exim: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Exim ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 26 Jul 2024

**[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 25 Jul 2024

**[NEU] [hoch] Mitel MiCollab: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Mitel MiCollab ausnutzen, um seine Privilegien zu erhöhen oder Code auszuführen.

- [Link](#)

—

Thu, 25 Jul 2024

***[NEU] [hoch] VMware Tanzu Spring Cloud: Schwachstelle ermöglicht Codeausführung***

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in VMware Tanzu Spring Cloud ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 25 Jul 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 25 Jul 2024

***[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting***

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- [Link](#)

—

Thu, 25 Jul 2024

***[UPDATE] [hoch] Linux Kernel (vmwgfx): Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 25 Jul 2024

***[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen***

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonym Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- [Link](#)

—

Thu, 25 Jul 2024

***[UPDATE] [hoch] Node.js: Mehrere Schwachstellen***

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine

Privilegien zu erweitern.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/27/2024	[Photon OS 3.0: Httpd PHSA-2024-3.0-0774]	critical
7/27/2024	[openSUSE 15 Security Update : python-nltk (openSUSE-SU-2024:0222-1)]	critical
7/27/2024	[Fedora 40 : darkhttpd (2024-25f8e34407)]	critical
7/27/2024	[CBL Mariner 2.0 Security Update: openssl (CVE-2024-5535)]	critical
7/27/2024	[Fedora 39 : darkhttpd (2024-d638b9a34c)]	critical
7/26/2024	[Rocky Linux 9 : httpd (RLSA-2024:4726)]	critical
7/26/2024	[Docker Engine < 23.0.15 / 26.x < 26.1.5 / 27.x < 27.1.1 Authentication Bypass]	critical
7/26/2024	[Progress Telerik Report Server Insecure Deserialization (CVE-2024-6327)]	critical
7/27/2024	[Photon OS 3.0: Vim PHSA-2022-3.0-0411]	high
7/27/2024	[Photon OS 3.0: Bluez PHSA-2024-3.0-0741]	high
7/27/2024	[Photon OS 3.0: Squid PHSA-2023-3.0-0689]	high
7/27/2024	[Photon OS 3.0: Squid PHSA-2024-3.0-0751]	high
7/27/2024	[Photon OS 5.0: Python3 PHSA-2024-5.0-0332]	high
7/27/2024	[openSUSE 15 Security Update : opera (openSUSE-SU-2024:0223-1)]	high
7/27/2024	[Fedora 40 : python-scrapy (2024-c27b82d702)]	high
7/27/2024	[CBL Mariner 2.0 Security Update: httpd (CVE-2024-40725)]	high
7/27/2024	[CBL Mariner 2.0 Security Update: httpd (CVE-2024-40898)]	high

Datum	Schwachstelle	Bewertung
7/27/2024	[CBL Mariner 2.0 Security Update: python-idna (CVE-2024-3651)]	high
7/27/2024	[Fedora 39 : python-scrapy (2024-0bd3b1212e)]	high
7/26/2024	[Rocky Linux 9 : skopeo (RLSA-2024:4502)]	high
7/26/2024	[Rocky Linux 9 : libndp (RLSA-2024:4636)]	high
7/26/2024	[Rocky Linux 8 / 9 : java-21-openjdk (RLSA-2024:4573)]	high
7/26/2024	[Atlassian Bamboo < 9.2.16 / < 9.6.4 File Inclusion (CVE-2024-21687)]	high
7/26/2024	[Apache CXF < 3.5.9, 3.6.x < 3.6.4, 4.0.x < 4.0.5 Multiple Vulnerabilities]	high
7/26/2024	[Apache CXF 3.6.x < 3.6.4, 4.0.x < 4.0.5 DoS]	high
7/26/2024	[Progress Telerik Reporting < 2024 Q2 (18.1.24.709) Object Injection]	high
7/26/2024	[TeamViewer < 15.52 Insecure Symlink Following (tv-2024-1002)]	high
7/26/2024	[Python Library Certifi < 2024.07.04 Untrusted Root Certificate]	high
7/26/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6917-1)]	high
7/26/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-6919-1)]	high
7/26/2024	[Ubuntu 24.04 LTS : Linux kernel vulnerabilities (USN-6918-1)]	high
7/26/2024	[FreeBSD : Mailpit – Content Security Policy XSS (3e917407-4b3f-11ef-8e49-001999f8d30b)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Thu, 25 Jul 2024

#### ***Prison Management System 1.0 Shell Upload***

Prison Management System version 1.0 suffers from an unauthenticated remote shell upload vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

#### ***Multi Store Inventory Management System 1.0 Insecure Direct Object Reference***

Multi Store Inventory Management System version 1.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

#### ***Online Medicine Ordering System 1.0 Insecure Settings***

Online Medicine Ordering System version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

#### ***Online Discussion Forum Site 1.0 Insecure Settings***

Online Discussion Forum Site version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

#### ***LMS ZAI 6.3 Insecure Settings***

LMS ZAI version 6.3 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

#### ***Ingredient Stock Management System 1.0 Insecure Settings***

Ingredient Stock Management System version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

***ChatBot Application With A Suggestion Feature 1.0 Insecure Settings***

ChatBot Application with a Suggestion Feature version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 25 Jul 2024

***Bhojon Restaurant Management System 2.7 Insecure Direct Object Reference***

Bhojon restaurant management system version 2.7 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Wed, 24 Jul 2024

***SIM Wisuda 1.0 Insecure Direct Object Reference***

SIM Wisuda version 1.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Wed, 24 Jul 2024

***SLiMS CMS 2.0 SQL Injection***

SLiMS CMS version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Wed, 24 Jul 2024

***StarTask CRM 1.9 SQL Injection***

StarTask CRM version 1.9 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Wed, 24 Jul 2024

***UBM CMS 1.2 Insecure Direct Object Reference***

UBM CMS version 1.2 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Wed, 24 Jul 2024

***TAIF LMS 5.8.0 Shell Upload***

TAIF LMS version 5.8.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Wed, 24 Jul 2024

**Vencorp 2.1.1 SQL Injection**

Vencorp version 2.1.1 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Wed, 24 Jul 2024

**Webdenim AppUI 1.0 Insecure Direct Object Reference**

Webdenim AppUI version 1.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Tue, 23 Jul 2024

**Perten Instruments Process Plus Software 1.11.6507.0 LFI / Hardcoded Credentials**

Perten Instruments Process Plus Software versions 1.11.6507.0 and below suffer from local file inclusion, hardcoded credential, and execution with unnecessary privilege vulnerabilities.

- [Link](#)

—

” “Tue, 23 Jul 2024

**LMS ZAI 6.1 Insecure Settings**

LMS ZAI version 6.1 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Tue, 23 Jul 2024

**Quick Job 2.4 Insecure Direct Object Reference**

Quick Job version 2.4 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Tue, 23 Jul 2024

**PPDB ONLINE 1.3 Administrative Page Disclosure**

PPDB ONLINE version 1.3 appears to suffer from an administrative page disclosure issue.

- [Link](#)

—

” “Tue, 23 Jul 2024

**PHP MaXiMuS 2.5.2 Cross Site Scripting**

PHP MaXiMuS version 2.5.2 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 23 Jul 2024



**NUKE SENTINEL 2.5.2 Cross Site Scripting**

NUKE SENTINEL version 2.5.2 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 23 Jul 2024

**Minfotech CMS 2.0 SQL Injection**

Minfotech CMS version 2.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 23 Jul 2024

**eDesign CMS 2.0 Insecure Direct Object Reference**

eDesign CMS version 2.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Mon, 22 Jul 2024

**Softing Secure Integration Server 1.22 Remote Code Execution**

This Metasploit module chains two vulnerabilities to achieve authenticated remote code execution against Softing Secure Integration Server version 1.22. In CVE-2022-1373, the restore configuration feature is vulnerable to a directory traversal vulnerability when processing zip files. When using the "restore configuration" feature to upload a zip file containing a path traversal file which is a dll called `..\..\..\..\..\..\..\..\..\..\Windows\System32\wbem\wbemcomn.dll`. This causes the file `C:\Windows\System32\wbem\wbemcomn.dll` to be created and executed upon touching the disk. In CVE-2022-2334, the planted `wbemcomn.dll` is used in a DLL hijacking attack when Softing Secure Integration Server restarts upon restoring configuration, which allows us to execute arbitrary code on the target system. The chain demonstrated in Pwn2Own used a signature instead of a password. The signature was acquired by running an ARP spoofing attack against the local network where the Softing SIS server was located. A username is also required for signature authentication. A custom DLL can be provided to use in the exploit instead of using the default MSF-generated one.

- [Link](#)

—

” “Mon, 22 Jul 2024

**Ghostscript Command Execution / Format String**

This Metasploit module exploits a format string vulnerability in Ghostscript versions before 10.03.1 to achieve a SAFER sandbox bypass and execute arbitrary commands. This vulnerability is reachable via libraries such as ImageMagick. This exploit only works against Ghostscript versions 10.03.0 and 10.01.2. Some offsets adjustment will probably be needed to make it work with other versions.

- [Link](#)

—

»

## 4.2 0-Days der letzten 5 Tage

“Fri, 26 Jul 2024

**ZDI-24-974: IrfanView CIN File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-973: IrfanView CIN File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-972: IrfanView AWD File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-971: IrfanView PSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-970: IrfanView PSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-969: IrfanView PSP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-968: IrfanView PSP File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-967: IrfanView RLE File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-966: Docker Desktop Daemon CLI External Control of File Path Denial-of-Service Vulnerability**

- [Link](#)

—

” “Fri, 26 Jul 2024

**ZDI-24-965: Apple macOS VideoToolbox Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

**ZDI-24-964: Autodesk AutoCAD STEP File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

**ZDI-24-963: Autodesk AutoCAD X\_T File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

**ZDI-24-962: Autodesk AutoCAD X\_T File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

**ZDI-24-961: Autodesk AutoCAD X\_B File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

**ZDI-24-960: Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

**ZDI-24-959: Autodesk AutoCAD X\_T File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 25 Jul 2024

***ZDI-24-958: Autodesk AutoCAD X\_T File Parsing Out-Of-Bounds Read 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: (Jul)

Datum	Opfer	Land	Information
2024-07-25	Summerville	[USA]	<a href="#">Link</a>
2024-07-24	Département des transports routiers de Selangor	[MYS]	<a href="#">Link</a>
2024-07-23	Red Art Games	[FRA]	<a href="#">Link</a>
2024-07-23	Ville de Cold Lake	[CAN]	<a href="#">Link</a>
2024-07-23	Gouvernement brésilien	[BRA]	<a href="#">Link</a>
2024-07-23	Dibulla	[COL]	<a href="#">Link</a>
2024-07-22	Aéroport de Split	[HRV]	<a href="#">Link</a>
2024-07-22	Forest Park	[USA]	<a href="#">Link</a>
2024-07-22	Jefferson County Clerk's Office	[USA]	<a href="#">Link</a>
2024-07-20	Melchers	[SGP]	<a href="#">Link</a>
2024-07-19	Le Tribunal supérieur du comté de Los Angeles	[USA]	<a href="#">Link</a>
2024-07-18	Cadastre hellénique	[GRC]	<a href="#">Link</a>
2024-07-18	Casino du Grand Cercle	[FRA]	<a href="#">Link</a>
2024-07-18	Globes	[ISR]	<a href="#">Link</a>
2024-07-18	Ville de Columbus	[USA]	<a href="#">Link</a>
2024-07-18	Wattle Range Council	[AUS]	<a href="#">Link</a>
2024-07-17	Ingemmet	[PER]	<a href="#">Link</a>
2024-07-16	Le Département de Loire-Atlantique	[FRA]	<a href="#">Link</a>
2024-07-16	Les Transports Publics du Chablais (TPC)	[CHE]	<a href="#">Link</a>
2024-07-15	Department of Migrant Workers (DMW)	[PHL]	<a href="#">Link</a>
2024-07-15	Cadre Holdings, Inc.	[USA]	<a href="#">Link</a>
2024-07-14	Metalfrio	[BRA]	<a href="#">Link</a>
2024-07-14	MERB	[DEU]	<a href="#">Link</a>
2024-07-13	AKG	[DEU]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-07-12	Sesc Tocantins	[BRA]	<a href="#">Link</a>
2024-07-12	ValeCard	[BRA]	<a href="#">Link</a>
2024-07-11	Allegheny County District Attorney's Office	[USA]	<a href="#">Link</a>
2024-07-11	Solutions&Co	[FRA]	<a href="#">Link</a>
2024-07-10	Jaboatão dos Guararapes	[BRA]	<a href="#">Link</a>
2024-07-10	Sibanye Stillwater	[ZAF]	<a href="#">Link</a>
2024-07-10	District scolaire de Goshen	[USA]	<a href="#">Link</a>
2024-07-10	Bassett Furniture Industries Inc.	[USA]	<a href="#">Link</a>
2024-07-10	Active Learning Trust	[GBR]	<a href="#">Link</a>
2024-07-10	Oxfam Hong Kong	[HKG]	<a href="#">Link</a>
2024-07-09	Clay County Courthouse	[USA]	<a href="#">Link</a>
2024-07-09	Ville de Mahina	[FRA]	<a href="#">Link</a>
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	<a href="#">Link</a>
2024-07-04	La Ville d'Ans	[BEL]	<a href="#">Link</a>
2024-07-04	Alps Alpine	[CHN]	<a href="#">Link</a>
2024-07-03	E.S.E. Salud Yopal	[COL]	<a href="#">Link</a>
2024-07-03	Florida Department of Health	[USA]	<a href="#">Link</a>
2024-07-03	Southwest Tennessee Community College (SWTCC)	[USA]	<a href="#">Link</a>
2024-07-02	Hong Kong Institute of Architects	[HKG]	<a href="#">Link</a>
2024-07-02	Apex	[USA]	<a href="#">Link</a>
2024-07-01	Hiap Seng Industries	[SGP]	<a href="#">Link</a>
2024-07-01	Monroe County government	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-28	[intrama-bg]	stormous	<a href="#">Link</a>
2024-07-27	[hanoverhill.com]	blacksuit	<a href="#">Link</a>
2024-07-27	[New Jersey City University]	rhysida	<a href="#">Link</a>
2024-07-25	[glnf.fr]	lockbit3	<a href="#">Link</a>
2024-07-27	[Computer Networking Solutions]	rhysida	<a href="#">Link</a>
2024-07-26	[ayurcan]	qilin	<a href="#">Link</a>
2024-07-27	[Kalaswire.com]	cloak	<a href="#">Link</a>
2024-07-26	[Community Care Alliance]	rhysida	<a href="#">Link</a>
2024-07-22	[www.neurologicalinstitute.com]	ransomhub	<a href="#">Link</a>
2024-07-26	[www.whittakersystem.com]	ransomhub	<a href="#">Link</a>
2024-07-26	[www.castelligroup.com]	ransomhub	<a href="#">Link</a>
2024-07-26	[City of Cold Lake]	fog	<a href="#">Link</a>
2024-07-26	[pioneerworldwide.com]	embargo	<a href="#">Link</a>
2024-07-26	[summervillepolice.com]	embargo	<a href="#">Link</a>
2024-07-26	[blankstyle.com]	darkvault	<a href="#">Link</a>
2024-07-26	[Augusta Orthopedic]	bianlian	<a href="#">Link</a>
2024-07-26	[Karvo Companies, Inc.]	bianlian	<a href="#">Link</a>
2024-07-26	[Planet Group International]	ransomexx	<a href="#">Link</a>
2024-07-26	[LITEON]	ransomexx	<a href="#">Link</a>
2024-07-26	[Texas Tech University]	meow	<a href="#">Link</a>
2024-07-26	[Global Industry Analysts]	meow	<a href="#">Link</a>
2024-07-26	[Encore]	meow	<a href="#">Link</a>
2024-07-26	[Daikin]	meow	<a href="#">Link</a>
2024-07-26	[Miami Gardens Florida]	meow	<a href="#">Link</a>
2024-07-26	[Nuclep]	meow	<a href="#">Link</a>
2024-07-26	[Andersen Tax]	meow	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-26	[The Physical Medicine Rehabilitation Center]	meow	<a href="#">Link</a>
2024-07-26	[Villarreal and Begum Law Firm]	meow	<a href="#">Link</a>
2024-07-23	[ach.co.th]	ransomhub	<a href="#">Link</a>
2024-07-23	[bpjaguar.com]	ransomhub	<a href="#">Link</a>
2024-07-24	[oficina.oficinadasfinancas.com.br]	ransomhub	<a href="#">Link</a>
2024-07-26	[Innovalve 3TB Data Leak ( \$300M )]	handala	<a href="#">Link</a>
2024-07-26	[Speed Advisory]	everest	<a href="#">Link</a>
2024-07-25	[mrhme.org]	ransomhub	<a href="#">Link</a>
2024-07-25	[The Computer Merchant]	play	<a href="#">Link</a>
2024-07-25	[Williams Construction]	play	<a href="#">Link</a>
2024-07-25	[Gateway Extrusions]	play	<a href="#">Link</a>
2024-07-25	[Physical & Occupational Therapy Examiners of Texas]	hunters	<a href="#">Link</a>
2024-07-25	[panitchlaw.com]	ransomhub	<a href="#">Link</a>
2024-07-25	[cminsulation.com]	ransomhub	<a href="#">Link</a>
2024-07-25	[baytoti.com]	ransomhub	<a href="#">Link</a>
2024-07-25	[Gendron & Gendron]	play	<a href="#">Link</a>
2024-07-25	[Golden Business Machines]	play	<a href="#">Link</a>
2024-07-25	[Odyssey Fitness Center]	play	<a href="#">Link</a>
2024-07-25	[OfficeOps]	play	<a href="#">Link</a>
2024-07-25	[BK Aerospace]	dragonforce	<a href="#">Link</a>
2024-07-25	[D&K Group, Inc.]	cicada3301	<a href="#">Link</a>
2024-07-25	[Voss Belting & Specialty]	cicada3301	<a href="#">Link</a>
2024-07-25	[Tri-Star Display]	cicada3301	<a href="#">Link</a>
2024-07-25	[NARSTCO]	cicada3301	<a href="#">Link</a>
2024-07-25	[Odessa College]	fog	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-25	[orbinox.com]	madliberator	Link
2024-07-15	[KMLG]	qilin	<a href="#">Link</a>
2024-07-23	[EHS Partnerships]	qilin	<a href="#">Link</a>
2024-07-25	[Environmental DesignInternational]	akira	Link
2024-07-25	[Empereon Constar]	akira	Link
2024-07-17	[Northern Bedford County School District (nbcsc.org)]	incransom	Link
2024-07-25	[Physical & Occupational Therapy Examiners ofTexas]	hunters	<a href="#">Link</a>
2024-07-25	[CertiCon]	dragonforce	<a href="#">Link</a>
2024-07-25	[SOLOMONUS.COM]	clop	Link
2024-07-25	[Insula Group]	bianlian	Link
2024-07-22	[tccfleet.com]	lockbit3	Link
2024-07-24	[petroassist.co.uk]	lockbit3	Link
2024-07-24	[e21c.co.uk]	lockbit3	Link
2024-07-23	[Owens Valley Career Development Center]	medusa	Link
2024-07-23	[Coffrage LD]	medusa	Link
2024-07-24	[Vivara]	medusa	Link
2024-07-25	[crimsonwinegroup.com]	abyss	Link
2024-07-24	[Stienemann]	spacebears	<a href="#">Link</a>
2024-07-25	[Pojoaque]	blacksuit	<a href="#">Link</a>
2024-07-24	[Kusum Group of Companies]	raworld	Link
2024-07-24	[TheLutheranFoundation]	raworld	Link
2024-07-24	[Melchers Singapore]	raworld	Link
2024-07-20	[Valisana]	ransomhouse	<a href="#">Link</a>
2024-07-24	[simple-solution-systems]	qilin	<a href="#">Link</a>
2024-07-24	[Bunkhouse Group]	bianlian	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-24	[Playa Vista Job Opportunities and Business Services]	bianlian	<a href="#">Link</a>
2024-07-24	[Accelon Technologies Private]	bianlian	<a href="#">Link</a>
2024-07-24	[SKC West]	akira	<a href="#">Link</a>
2024-07-24	[ORBINOX]	madliberator	<a href="#">Link</a>
2024-07-24	[vrd.be]	madliberator	<a href="#">Link</a>
2024-07-24	[Betances Health Center]	hunters	<a href="#">Link</a>
2024-07-23	[BLEnergy]	handala	<a href="#">Link</a>
2024-07-24	[Jack “Designer” Sparrow.]	donutleaks	<a href="#">Link</a>
2024-07-24	[American Acryl]	akira	<a href="#">Link</a>
2024-07-24	[Electroalfa]	akira	<a href="#">Link</a>
2024-07-24	[CALDAN Conveyor]	akira	<a href="#">Link</a>
2024-07-24	[forestparkga.gov]	monti	<a href="#">Link</a>
2024-07-24	[Regas (regasenergy.com)]	monti	<a href="#">Link</a>
2024-07-24	[Dimbleby Funeral Homes]	dragonforce	<a href="#">Link</a>
2024-07-24	[John Gallin & Son]	dragonforce	<a href="#">Link</a>
2024-07-24	[Industrial Bolsera]	donutleaks	<a href="#">Link</a>
2024-07-24	[RhinoCorps]	blacksuit	<a href="#">Link</a>
2024-07-17	[Congoleum]	play	<a href="#">Link</a>
2024-07-23	[sigmacontrol.eu]	ransomhub	<a href="#">Link</a>
2024-07-23	[siParadigm]	akira	<a href="#">Link</a>
2024-07-23	[eurovilla.hr]	darkvault	<a href="#">Link</a>
2024-07-23	[Notarkammer Pfalz]	akira	<a href="#">Link</a>
2024-07-23	[Win Systems]	akira	<a href="#">Link</a>
2024-07-20	[www.byzan.com]	ransomhub	<a href="#">Link</a>
2024-07-16	[maingroup]	incransom	<a href="#">Link</a>
2024-07-08	[Cedar Technologies]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-12	[American Golf ]	medusa	<a href="#">Link</a>
2024-07-15	[Royal Brighton Yacht Club]	medusa	<a href="#">Link</a>
2024-07-15	[ValeCard]	medusa	<a href="#">Link</a>
2024-07-16	[H&H Group]	medusa	<a href="#">Link</a>
2024-07-16	[Jarjet Technologies]	medusa	<a href="#">Link</a>
2024-07-22	[Globes]	medusa	<a href="#">Link</a>
2024-07-22	[AA Munro Insurance]	medusa	<a href="#">Link</a>
2024-07-23	[thesourcinggroup.com]	dAn0n	<a href="#">Link</a>
2024-07-23	[LawDepot]	rhysida	<a href="#">Link</a>
2024-07-23	[Association Management Strategies(AAMC.local)]	incransom	<a href="#">Link</a>
2024-07-08	[CIMP.COM]	incransom	<a href="#">Link</a>
2024-07-22	[Wichita State University Campus of Applied Sciences and Technology]	fog	<a href="#">Link</a>
2024-07-22	[memc.com]	blackbasta	<a href="#">Link</a>
2024-07-22	[SH Pension]	everest	<a href="#">Link</a>
2024-07-11	[Sibanye-Stillwater]	ransomhouse	<a href="#">Link</a>
2024-07-22	[Acadian Ambulance (US)]	daixin	<a href="#">Link</a>
2024-07-21	[Sherbrooke Metals]	BrainCipher	<a href="#">Link</a>
2024-07-21	[Apex Global	Big leak outlooks - 2tb.]	BrainCipher
2024-07-21	[Cole Technologies Group]	BrainCipher	<a href="#">Link</a>
2024-07-21	[Family Wealth Advisors Ltd.]	BrainCipher	<a href="#">Link</a>
2024-07-21	[Mars 2 LLC]	BrainCipher	<a href="#">Link</a>
2024-07-21	[KickDown ESET company. No overpayments at 0% (renamed and update)]	donutleaks	<a href="#">Link</a>
2024-07-21	[Handala's attack on Israeli organizations]	handala	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-20	[Queens County Public Administrator]	rhysida	<a href="#">Link</a>
2024-07-20	[www.garudafood.com]	ransomhub	<a href="#">Link</a>
2024-07-20	[Reward Hospitality from EFC Group]	blacksuit	<a href="#">Link</a>
2024-07-20	[ESET. PREMIUM.]	donutleaks	<a href="#">Link</a>
2024-07-20	[Doodle Tech]	arcusmedia	<a href="#">Link</a>
2024-07-19	[www.kumagaigumi.co.jp]	ransomhub	<a href="#">Link</a>
2024-07-19	[Arcmed Group]	hunters	<a href="#">Link</a>
2024-07-19	[Leech Lake Gaming]	cicada3301	<a href="#">Link</a>
2024-07-15	[concorddirect.com]	lockbit3	<a href="#">Link</a>
2024-07-15	[townandforest.co.uk]	lockbit3	<a href="#">Link</a>
2024-07-17	[norton.k12.ma.us]	lockbit3	<a href="#">Link</a>
2024-07-17	[energateinc.com]	lockbit3	<a href="#">Link</a>
2024-07-17	[plantmachineworks.com]	lockbit3	<a href="#">Link</a>
2024-07-17	[piedmonthoist.com]	lockbit3	<a href="#">Link</a>
2024-07-17	[gptchb.org]	lockbit3	<a href="#">Link</a>
2024-07-17	[assih.com]	lockbit3	<a href="#">Link</a>
2024-07-18	[wattlerange.sa.gov.au]	lockbit3	<a href="#">Link</a>
2024-07-18	[claycountyin.gov]	lockbit3	<a href="#">Link</a>
2024-07-18	[iteam.gr]	lockbit3	<a href="#">Link</a>
2024-07-18	[albonanova.at]	lockbit3	<a href="#">Link</a>
2024-07-18	[lothar-rapp.de]	lockbit3	<a href="#">Link</a>
2024-07-18	[goldstarmetal.com]	lockbit3	<a href="#">Link</a>
2024-07-18	[glsco.com]	lockbit3	<a href="#">Link</a>
2024-07-18	[paysdelaloire.fr]	lockbit3	<a href="#">Link</a>
2024-07-18	[troyareasd.org]	lockbit3	<a href="#">Link</a>
2024-07-18	[barkingwell.gr]	lockbit3	<a href="#">Link</a>
2024-07-18	[fbrlaw.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-18	[customssupport.be]	lockbit3	<a href="#">Link</a>
2024-07-18	[joliet86.org]	lockbit3	<a href="#">Link</a>
2024-07-16	[www.glowfm.nl]	ransomhub	<a href="#">Link</a>
2024-07-19	[Law Offices of the Public Defender - New Mexico]	rhysida	<a href="#">Link</a>
2024-07-05	[Infomedika]	ransomhouse	<a href="#">Link</a>
2024-07-17	[Next step healthcar]	qilin	<a href="#">Link</a>
2024-07-18	[Northeast Rehabilitation Hospital Network]	hunters	<a href="#">Link</a>
2024-07-18	[Seamon Whiteside]	hunters	<a href="#">Link</a>
2024-07-18	[Santa Rosa]	hunters	<a href="#">Link</a>
2024-07-18	[all-mode.com]	donutleaks	<a href="#">Link</a>
2024-07-14	[www.erma-rtmo.it]	ransomhub	<a href="#">Link</a>
2024-07-16	[metalfrio.com.br]	ransomhub	<a href="#">Link</a>
2024-07-16	[www.newcastlewa.gov]	ransomhub	<a href="#">Link</a>
2024-07-18	[pgd.pl]	ransomhub	<a href="#">Link</a>
2024-07-17	[Modernauto]	blackbyte	<a href="#">Link</a>
2024-07-17	[Modern Automotive Group]	blackbyte	<a href="#">Link</a>
2024-07-17	[Gandara Center]	rhysida	<a href="#">Link</a>
2024-07-17	[C???o???m]	play	<a href="#">Link</a>
2024-07-17	[Hayden Power Group]	play	<a href="#">Link</a>
2024-07-17	[MIPS Technologies]	play	<a href="#">Link</a>
2024-07-17	[ZSZAALJL.cz]	qilin	<a href="#">Link</a>
2024-07-17	[Eyal Baror the key official of the 8200 unit]	handala	<a href="#">Link</a>
2024-07-17	[labline.it]	donutleaks	<a href="#">Link</a>
2024-07-16	[www.hlbpr.com]	ransomhub	<a href="#">Link</a>
2024-07-17	[isometrix.com]	cactus	<a href="#">Link</a>
2024-07-06	[A.L.P. Lighting Components]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-16	[VITALDENT]	madliberator	<a href="#">Link</a>
2024-07-12	[BENICULTURALI.IT]	madliberator	<a href="#">Link</a>
2024-07-12	[MONTERO & SEGURA]	madliberator	<a href="#">Link</a>
2024-07-12	[crosswear.co.uk]	madliberator	<a href="#">Link</a>
2024-07-12	[sacities.net]	madliberator	<a href="#">Link</a>
2024-07-17	[zb.co.zw]	madliberator	<a href="#">Link</a>
2024-07-17	[The Law Office of Omar O. Vargas, P.C.]	everest	<a href="#">Link</a>
2024-07-17	[STUDIO NOTARILE BUCCI – OLMI]	everest	<a href="#">Link</a>
2024-07-16	[GroupePRO-B]	cicada3301	<a href="#">Link</a>
2024-07-16	[Greenheck]	meow	<a href="#">Link</a>
2024-07-16	[CBIZ Inc]	meow	<a href="#">Link</a>
2024-07-16	[Hewlett Packard Enterprise]	meow	<a href="#">Link</a>
2024-07-16	[BCS Systems]	meow	<a href="#">Link</a>
2024-07-16	[Guhring]	meow	<a href="#">Link</a>
2024-07-16	[Odfjell Drilling]	meow	<a href="#">Link</a>
2024-07-16	[Golan Christie Taglia]	meow	<a href="#">Link</a>
2024-07-16	[First Commonwealth Federal Credit Union]	meow	<a href="#">Link</a>
2024-07-07	[Djg Projects]	fog	<a href="#">Link</a>
2024-07-04	[Verweij Elektrotechniek]	fog	<a href="#">Link</a>
2024-07-04	[Alvin Independent School District]	fog	<a href="#">Link</a>
2024-07-11	[West Allis-West Milwaukee School District]	fog	<a href="#">Link</a>
2024-07-16	[German University of Technology in Oman]	fog	<a href="#">Link</a>
2024-07-16	[ceopag.com.br / ceofood.com.br]	ransomhub	<a href="#">Link</a>
2024-07-16	[[temporary] Warning for Eyal Baror]	handala	<a href="#">Link</a>
2024-07-16	[www.benchinternational.com]	ransomhub	<a href="#">Link</a>
2024-07-16	[www.cameronhodes.com]	ransomhub	<a href="#">Link</a>
2024-07-16	[Braum's Inc]	hunters	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-16	[Lantronix Inc.]	hunters	<a href="#">Link</a>
2024-07-16	[HOYA Corporation]	hunters	<a href="#">Link</a>
2024-07-16	[Mainland Machinery]	dragonforce	<a href="#">Link</a>
2024-07-16	[SBRPCA]	dragonforce	<a href="#">Link</a>
2024-07-16	[verco.co.uk]	cactus	<a href="#">Link</a>
2024-07-15	[Nuevatel]	dunghill	<a href="#">Link</a>
2024-07-15	[Innovalve Bio Medical]	handala	<a href="#">Link</a>
2024-07-09	[www.baiminstitute.org]	ransomhub	<a href="#">Link</a>
2024-07-13	[integraservices]	mallox	<a href="#">Link</a>
2024-07-14	[XENAPP-GLOBER]	mallox	<a href="#">Link</a>
2024-07-15	[Gramercy Surgery Center]	everest	<a href="#">Link</a>
2024-07-15	[posiplus.com]	blackbasta	<a href="#">Link</a>
2024-07-15	[hpecds.com]	blackbasta	<a href="#">Link</a>
2024-07-15	[Amino Transport]	akira	<a href="#">Link</a>
2024-07-15	[Goede, DeBoest & Cross, PLLC.]	rhysida	<a href="#">Link</a>
2024-07-15	[Sheba Medical Center]	handala	<a href="#">Link</a>
2024-07-15	[usdermpartners.com]	blackbasta	<a href="#">Link</a>
2024-07-15	[atos.com]	blackbasta	<a href="#">Link</a>
2024-07-15	[Gibbs Hurley Chartered Accountants]	hunters	<a href="#">Link</a>
2024-07-15	[ComNet Communications]	hunters	<a href="#">Link</a>
2024-07-15	[MS Ultrasonic Technology Group]	hunters	<a href="#">Link</a>
2024-07-15	[RZO]	hunters	<a href="#">Link</a>
2024-07-15	[thompsoncreek.com_wa]	blackbasta	<a href="#">Link</a>
2024-07-15	[northernsafety.com_wa]	blackbasta	<a href="#">Link</a>
2024-07-15	[upcli.com]	cloak	<a href="#">Link</a>
2024-07-15	[greenlightbiosciences.com]	abyss	<a href="#">Link</a>
2024-07-15	[valleylandtitleco.com - UPD]	donutleaks	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-14	[luzan5.com]	blackout	<a href="#">Link</a>
2024-07-14	[BrownWinick]	rhysida	<a href="#">Link</a>
2024-07-14	[Texas Alcohol & Drug Testing Service]	bianlian	<a href="#">Link</a>
2024-07-13	[a-g.com - data publication 38gb (150K)]	blacksuit	<a href="#">Link</a>
2024-07-13	[gbhs.org Publication 51gb]	blacksuit	<a href="#">Link</a>
2024-07-13	[Kenya Urban Roads Authority]	hunters	<a href="#">Link</a>
2024-07-13	[Carigali Hess Operating Company]	hunters	<a href="#">Link</a>
2024-07-13	[gbhs.org 07/12 Publication 51gb]	blacksuit	<a href="#">Link</a>
2024-07-01	[The Coffee Bean & Tea Leaf]	incransom	<a href="#">Link</a>
2024-07-01	[State of Alabama - Alabama Department Of Education]	incransom	<a href="#">Link</a>
2024-07-02	[ARISTA]	spacebears	<a href="#">Link</a>
2024-07-12	[Preferred IT Group]	bianlian	<a href="#">Link</a>
2024-07-08	[Wagner-Meinert]	ransomexx	<a href="#">Link</a>
2024-07-12	[painproclinics.com]	ransomcortex	<a href="#">Link</a>
2024-07-02	[www.zepter.de]	ransomhub	<a href="#">Link</a>
2024-07-11	[www.riteaid.com]	ransomhub	<a href="#">Link</a>
2024-07-03	[olympusgrp.com]	dispossessor	<a href="#">Link</a>
2024-07-12	[www.donaanita.com]	ransomcortex	<a href="#">Link</a>
2024-07-12	[perfeitaplastica.com.br]	ransomcortex	<a href="#">Link</a>
2024-07-12	[www.respirarlondrina.com.br]	ransomcortex	<a href="#">Link</a>
2024-07-11	[Hyperice]	play	<a href="#">Link</a>
2024-07-11	[diligentusa.com]	embargo	<a href="#">Link</a>
2024-07-11	[Image Microsystems]	blacksuit	<a href="#">Link</a>
2024-07-11	[www.lynchaluminum.com]	ransomhub	<a href="#">Link</a>
2024-07-11	[www.eurostrand.de]	ransomhub	<a href="#">Link</a>
2024-07-11	[www.netavent.dk]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-11	[Financoop]	akira	<a href="#">Link</a>
2024-07-11	[Sigma]	akira	<a href="#">Link</a>
2024-07-11	[Sonol ( Gas Stations )]	handala	<a href="#">Link</a>
2024-07-11	[www.bfcsolutions.com]	ransomhub	<a href="#">Link</a>
2024-07-11	[Texas Electric Cooperatives]	play	<a href="#">Link</a>
2024-07-11	[The 21st Century Energy Group]	play	<a href="#">Link</a>
2024-07-11	[T P C I]	play	<a href="#">Link</a>
2024-07-10	[City of Cedar Falls]	blacksuit	<a href="#">Link</a>
2024-07-10	[P448]	akira	<a href="#">Link</a>
2024-07-10	[Beowulfchain]	vanirgroup	<a href="#">Link</a>
2024-07-10	[Qinao]	vanirgroup	<a href="#">Link</a>
2024-07-10	[Athlon]	vanirgroup	<a href="#">Link</a>
2024-07-10	[Usina Alta Mogiana S/A]	akira	<a href="#">Link</a>
2024-07-09	[Inland Audio Visual]	akira	<a href="#">Link</a>
2024-07-09	[Indika Energy]	hunters	<a href="#">Link</a>
2024-07-08	[Excelsior Orthopaedics]	monti	<a href="#">Link</a>
2024-07-09	[Heidmar]	akira	<a href="#">Link</a>
2024-07-03	[REPLIGEN]	incransom	<a href="#">Link</a>
2024-07-08	[Raffmetal Spa]	dragonforce	<a href="#">Link</a>
2024-07-08	[Allied Industrial Group]	akira	<a href="#">Link</a>
2024-07-08	[Esedra]	akira	<a href="#">Link</a>
2024-07-08	[Federated Co-operatives]	akira	<a href="#">Link</a>
2024-07-02	[Guhring USA]	incransom	<a href="#">Link</a>
2024-07-06	[noab.nl]	lockbit3	<a href="#">Link</a>
2024-07-07	[Strauss Brands ]	medusa	<a href="#">Link</a>
2024-07-07	[Harry Perkins Institute of medical research ]	medusa	<a href="#">Link</a>
2024-07-07	[Viasat ]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-07	[Olympus Group]	medusa	<a href="#">Link</a>
2024-07-07	[MYC Media]	rhysida	<a href="#">Link</a>
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	<a href="#">Link</a>
2024-07-03	[baiminstitute.org]	ransomhub	<a href="#">Link</a>
2024-07-05	[The Wacks Law Group]	qilin	<a href="#">Link</a>
2024-07-05	[pomalca.com.pe]	qilin	<a href="#">Link</a>
2024-07-05	[Center for Human Capital Innovation (centerforhcci.org)]	incransom	<a href="#">Link</a>
2024-07-05	[waupacacounty-wi.gov]	incransom	<a href="#">Link</a>
2024-07-05	[waupaca.wi.us]	incransom	<a href="#">Link</a>
2024-07-04	[ws-stahl.eu]	lockbit3	<a href="#">Link</a>
2024-07-04	[homelandvinyl.com]	lockbit3	<a href="#">Link</a>
2024-07-04	[eicher.in]	lockbit3	<a href="#">Link</a>
2024-07-05	[National Health Laboratory Services]	blacksuit	<a href="#">Link</a>
2024-07-04	[Un Museau]	spacebears	<a href="#">Link</a>
2024-07-03	[Haylem]	spacebears	<a href="#">Link</a>
2024-07-04	[Elyria Foundry]	play	<a href="#">Link</a>
2024-07-04	[Texas Recycling]	play	<a href="#">Link</a>
2024-07-04	[INDA's]	play	<a href="#">Link</a>
2024-07-04	[Innerspec Technologies]	play	<a href="#">Link</a>
2024-07-04	[Prairie Athletic Club]	play	<a href="#">Link</a>
2024-07-04	[Fareri Associates]	play	<a href="#">Link</a>
2024-07-04	[Island Transportation Corp.]	bianlian	<a href="#">Link</a>
2024-07-04	[Legend Properties, Inc.]	bianlian	<a href="#">Link</a>
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	<a href="#">Link</a>
2024-07-03	[hcri.edu]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-04	[Coquitlam Concrete]	hunters	<a href="#">Link</a>
2024-07-04	[Multisuns Communication]	hunters	<a href="#">Link</a>
2024-07-04	[gerard-perrier.com]	embargo	<a href="#">Link</a>
2024-07-04	[Abileneisd.org]	cloak	<a href="#">Link</a>
2024-07-03	[sequelglobal.com]	darkvault	<a href="#">Link</a>
2024-07-03	[Explomin]	akira	<a href="#">Link</a>
2024-07-03	[Alimac]	akira	<a href="#">Link</a>
2024-07-03	[badel1862.hr]	blackout	<a href="#">Link</a>
2024-07-03	[ramservices.com]	underground	<a href="#">Link</a>
2024-07-03	[foremedia.net]	darkvault	<a href="#">Link</a>
2024-07-03	[www.swcs-inc.com]	ransomhub	<a href="#">Link</a>
2024-07-03	[valleylandtitleco.com]	donutleaks	<a href="#">Link</a>
2024-07-02	[merrymanhouse.org]	lockbit3	<a href="#">Link</a>
2024-07-02	[fairfieldmemorial.org]	lockbit3	<a href="#">Link</a>
2024-07-02	[www.daesangamerica.com]	ransomhub	<a href="#">Link</a>
2024-07-02	[P1 Technologies]	akira	<a href="#">Link</a>
2024-07-02	[Conexus Medstaff]	akira	<a href="#">Link</a>
2024-07-02	[Salton]	akira	<a href="#">Link</a>
2024-07-01	[www.sfmedical.de]	ransomhub	<a href="#">Link</a>
2024-07-02	[WheelerShip]	hunters	<a href="#">Link</a>
2024-07-02	[Grand Rapids Gravel]	dragonforce	<a href="#">Link</a>
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	<a href="#">Link</a>
2024-07-02	[Elite Fitness]	dragonforce	<a href="#">Link</a>
2024-07-02	[Gray & Adams]	dragonforce	<a href="#">Link</a>
2024-07-02	[Vermont Panurgy]	dragonforce	<a href="#">Link</a>
2024-07-01	[floridahealth.gov]	ransomhub	<a href="#">Link</a>
2024-07-01	[www.nttdata.ro]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-01	[Super Gardens]	dragonforce	<a href="#">Link</a>
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	<a href="#">Link</a>
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	<a href="#">Link</a>
2024-07-01	[SYNERGY PEANUT]	akira	<a href="#">Link</a>
2024-07-01	[Ethypharm]	underground	<a href="#">Link</a>
2024-07-01	[latinsa.co.id]	lockbit3	<a href="#">Link</a>
2024-07-01	[kbc-zagreb.hr]	lockbit3	<a href="#">Link</a>
2024-07-01	[maxcess-logistics.com]	killsec	<a href="#">Link</a>
2024-07-01	[Independent Education System]	handala	<a href="#">Link</a>
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	<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.