

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240828



## 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>12</b>
4.1 Exploits der letzten 5 Tage . . . . .	12
4.2 0-Days der letzten 5 Tage . . . . .	16
<b>5 Die Hacks der Woche</b>	<b>17</b>
5.0.1 AI ist nicht bereit für Production (Indirekte Prompt Injection in der Slack AI) . .	17
<b>6 Cyberangriffe: (Aug)</b>	<b>18</b>
<b>7 Ransomware-Erpressungen: (Aug)</b>	<b>19</b>
<b>8 Quellen</b>	<b>32</b>
8.1 Quellenverzeichnis . . . . .	32
<b>9 Impressum</b>	<b>34</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

#### ***Jetzt patchen! Netzwerksoftware Versa Director attackiert***

Derzeit nutzen Angreifer eine Schwachstelle in der Virtualisierungs- und Serviceerstellungsplattform Versa Director aus.

- [Link](#)

—

#### ***Wordpress: 1 Million Webseiten nutzen verwundbares Plug-in WPML***

Das Wordpress-Plug-in WPML kommt auf mehr als eine Million aktive Installationen. Jetzt wurde eine kritische Lücke darin gestopft.

- [Link](#)

—

#### ***Webbrowser: Weitere Lücke aktiv ausgenutzt, Adobe PDF-Viewer aktualisiert***

Google meldet das Ausnutzen einer weiteren Lücke in freier Wildbahn. Die Updates von Edge schließen auch ein Leck im Adobe PDF Viewer.

- [Link](#)

—

#### ***Notfall-Update: Microsoft behebt riskante Sicherheitslücke in Edge***

Google hat die Lücke im jüngsten Chrome-Update gepatcht, es gibt Hinweise auf aktive Exploits. Daher zieht Redmond nun nach.

- [Link](#)

—

#### ***Update verfügbar: IT-Sicherheitslösung IBM QRadar SIEM ist verwundbar***

IBM hat mehrere Sicherheitslücken in verschiedenen Komponenten von QRadar SIEM geschlossen.

- [Link](#)

—

#### ***Bamboo, Confluence, Jira und Co.: Atlassian schließt hochriskante Lücken***

Atlassian hat Updates für zahlreiche Produkte veröffentlicht. Sie schließen als hohes Risiko geltende Sicherheitslücken etwa in Bambo, Confluence und Jira.

- [Link](#)

—

#### ***Sicherheitsupdate: Attacken auf Sonicwall-Firewalls können Crash auslösen***

Um Netzwerke von Unternehmen zu schützen, sollten Admins ihre Firewalls von Sonicwall zeitnah auf den aktuellen Stand bringen.

- [Link](#)

—

***Hartkodierte Zugangsdaten gefährden Solarwinds Web Help Desk***

Angreifer können unbefugt auf die Kundensupport-Software Web Help Desk von Solarwinds zugreifen und Daten manipulieren.

- [Link](#)

—

***5 Millionen Wordpress-Seiten gefährdet: Kritisches Leck in LiteSpeed Cache***

Das Wordpress-Plug-in LiteSpeed Cache ist auf 5 Millionen Seiten installiert. Nun haben IT-Forscher eine kritische Sicherheitslücke darin entdeckt.

- [Link](#)

—

***Admin-Attacken auf GitHub Enterprise Server möglich***

Unter bestimmten Voraussetzungen können Angreifer Admin-Accounts von GitHub Enterprise Server kapern.

- [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-2023-6895	0.921160000	0.990050000	<a href="#">Link</a>
CVE-2023-6553	0.921020000	0.990030000	<a href="#">Link</a>
CVE-2023-6019	0.918710000	0.989810000	<a href="#">Link</a>
CVE-2023-5360	0.902780000	0.988800000	<a href="#">Link</a>
CVE-2023-52251	0.946410000	0.992890000	<a href="#">Link</a>
CVE-2023-4966	0.971280000	0.998330000	<a href="#">Link</a>
CVE-2023-49103	0.964030000	0.996060000	<a href="#">Link</a>
CVE-2023-48795	0.965330000	0.996460000	<a href="#">Link</a>
CVE-2023-47246	0.959760000	0.995180000	<a href="#">Link</a>
CVE-2023-46805	0.934240000	0.991480000	<a href="#">Link</a>
CVE-2023-46747	0.972900000	0.998920000	<a href="#">Link</a>
CVE-2023-46604	0.964990000	0.996310000	<a href="#">Link</a>
CVE-2023-4542	0.936770000	0.991690000	<a href="#">Link</a>
CVE-2023-43208	0.972610000	0.998780000	<a href="#">Link</a>
CVE-2023-43177	0.961750000	0.995550000	<a href="#">Link</a>
CVE-2023-42793	0.970220000	0.997900000	<a href="#">Link</a>
CVE-2023-41265	0.911110000	0.989330000	<a href="#">Link</a>
CVE-2023-39143	0.940480000	0.992100000	<a href="#">Link</a>
CVE-2023-38646	0.906950000	0.989050000	<a href="#">Link</a>
CVE-2023-38205	0.953670000	0.994150000	<a href="#">Link</a>
CVE-2023-38203	0.966410000	0.996740000	<a href="#">Link</a>
CVE-2023-38146	0.920720000	0.989990000	<a href="#">Link</a>
CVE-2023-38035	0.974690000	0.999720000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.966750000	0.996870000	<a href="#">Link</a>
CVE-2023-3519	0.965910000	0.996610000	<a href="#">Link</a>
CVE-2023-35082	0.967460000	0.997060000	<a href="#">Link</a>
CVE-2023-35078	0.970450000	0.997980000	<a href="#">Link</a>
CVE-2023-34993	0.973130000	0.999040000	<a href="#">Link</a>
CVE-2023-34960	0.928290000	0.990820000	<a href="#">Link</a>
CVE-2023-34634	0.925130000	0.990510000	<a href="#">Link</a>
CVE-2023-34362	0.970450000	0.997970000	<a href="#">Link</a>
CVE-2023-34039	0.952470000	0.993940000	<a href="#">Link</a>
CVE-2023-3368	0.937150000	0.991730000	<a href="#">Link</a>
CVE-2023-33246	0.972040000	0.998520000	<a href="#">Link</a>
CVE-2023-32315	0.970220000	0.997900000	<a href="#">Link</a>
CVE-2023-30625	0.953610000	0.994140000	<a href="#">Link</a>
CVE-2023-30013	0.965950000	0.996620000	<a href="#">Link</a>
CVE-2023-29300	0.969240000	0.997560000	<a href="#">Link</a>
CVE-2023-29298	0.941540000	0.992240000	<a href="#">Link</a>
CVE-2023-28432	0.911820000	0.989370000	<a href="#">Link</a>
CVE-2023-28343	0.933130000	0.991390000	<a href="#">Link</a>
CVE-2023-28121	0.919520000	0.989890000	<a href="#">Link</a>
CVE-2023-27524	0.970600000	0.998030000	<a href="#">Link</a>
CVE-2023-27372	0.973470000	0.999150000	<a href="#">Link</a>
CVE-2023-27350	0.969720000	0.997730000	<a href="#">Link</a>
CVE-2023-26469	0.951470000	0.993710000	<a href="#">Link</a>
CVE-2023-26360	0.963510000	0.995920000	<a href="#">Link</a>
CVE-2023-26035	0.969020000	0.997470000	<a href="#">Link</a>
CVE-2023-25717	0.954250000	0.994250000	<a href="#">Link</a>
CVE-2023-25194	0.967920000	0.997190000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996030000	<a href="#">Link</a>
CVE-2023-24489	0.973820000	0.999310000	<a href="#">Link</a>
CVE-2023-23752	0.956380000	0.994640000	<a href="#">Link</a>
CVE-2023-23333	0.962300000	0.995650000	<a href="#">Link</a>
CVE-2023-22527	0.968780000	0.997410000	<a href="#">Link</a>
CVE-2023-22518	0.965200000	0.996420000	<a href="#">Link</a>
CVE-2023-22515	0.972340000	0.998650000	<a href="#">Link</a>
CVE-2023-21839	0.955020000	0.994390000	<a href="#">Link</a>
CVE-2023-21554	0.955880000	0.994550000	<a href="#">Link</a>
CVE-2023-20887	0.970670000	0.998050000	<a href="#">Link</a>
CVE-2023-1671	0.964660000	0.996210000	<a href="#">Link</a>
CVE-2023-0669	0.969760000	0.997740000	<a href="#">Link</a>

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

Tue, 27 Aug 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Tue, 27 Aug 2024

#### **[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Windows, Microsoft Windows 10, Microsoft Windows 11, Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019 und Microsoft Windows Server 2022 ausnutzen, um beliebigen Programmcode auszuführen, beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)



—  
Tue, 27 Aug 2024

**[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, UI-Spoofing zu betreiben, Sicherheitsmechanismen zu umgehen und andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Tue, 27 Aug 2024

**[NEU] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform auf Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Mon, 26 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, 26 Aug 2024

**[NEU] [hoch] OTRS: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in OTRS ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Mon, 26 Aug 2024

**[UPDATE] [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](#)

—

Mon, 26 Aug 2024

**[UPDATE] [hoch] fetchmail: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in fetchmail ausnutzen, um einen Denial

of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Mon, 26 Aug 2024

**[UPDATE] [hoch] Mozilla Firefox und Firefox ESR: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- [Link](#)

—

Mon, 26 Aug 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](#)

—

Mon, 26 Aug 2024

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

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

- [Link](#)

—

Mon, 26 Aug 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](#)

—

Mon, 26 Aug 2024

**[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- [Link](#)

—

Fri, 23 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, 23 Aug 2024

**[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um falsche Informationen darzustellen und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 23 Aug 2024

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

Ein entfernter anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Fri, 23 Aug 2024

**[UPDATE] [hoch] ImageMagick: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ImageMagick ausnutzen, um einen Denial of Service Angriff durchzuführen oder um Informationen offenzulegen.

- [Link](#)

—

Fri, 23 Aug 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, 23 Aug 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—  
Fri, 23 Aug 2024

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

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

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/27/2024	[Progress WhatsUp Gold < 24.0.0 Multiple Vulnerabilities (000263015)]	critical
8/26/2024	[RHEL 9 : httpd (RHSA-2024:5832)]	critical
8/26/2024	[RHEL 7 : Red Hat JBoss Enterprise Application Platform 7.1.7 on RHEL 7 (RHSA-2024:5856)]	critical
8/26/2024	[RHEL 9 : httpd (RHSA-2024:5812)]	critical
8/27/2024	[SUSE SLES12 Security Update : xen (SUSE-SU-2024:3010-1)]	high
8/27/2024	[Debian dsa-5759 : idle-python3.11 - security update]	high
8/27/2024	[RHEL 7 : bind (RHSA-2024:5894)]	high
8/27/2024	[RHEL 8 : orc:0.4.28 (RHSA-2024:5882)]	high
8/27/2024	[RHEL 8 : krb5 (RHSA-2024:5884)]	high
8/27/2024	[RHEL 8 : libreoffice (RHSA-2024:5886)]	high
8/27/2024	[Fedora 40 : calibre (2024-a455bea9ca)]	high
8/27/2024	[Ubuntu 16.04 LTS : Drupal vulnerabilities (USN-6981-1)]	high
8/26/2024	[Debian dsa-5758 : trafficserver - security update]	high
8/26/2024	[RHEL 9 : kpatch-patch-5_14_0-70_85_1 (RHSA-2024:5858)]	high
8/26/2024	[RHEL 9 : bind and bind-dyndb-ldap (RHSA-2024:5813)]	high

Datum	Schwachstelle	Bewertung
8/26/2024	[RHEL 8 : bind (RHSA-2024:5838)]	high
8/26/2024	[CBL Mariner 2.0 Security Update: python-urllib3 (CVE-2023-43804)]	high
8/26/2024	[Ubuntu 18.04 LTS : Linux kernel (AWS) vulnerabilities (USN-6973-3)]	high
8/26/2024	[RHEL 8 : bind (RHSA-2024:5871)]	high
8/25/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0258-2)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Tue, 27 Aug 2024

#### **Linux lock\_get\_status() Use-After-Free**

An LSM can prevent the fcntl/close race cleanup path in fcntl\_setlk() from working, leading to use-after-free read in lock\_get\_status() when reading /proc/locks.

- [Link](#)

—

” “Tue, 27 Aug 2024

#### **PowerVR DevmemIntChangeSparse2() Use-After-Free**

PowerVR suffers from a use-after-free vulnerability in DevmemIntChangeSparse2() on a PMRGetUID() call.

- [Link](#)

—

” “Tue, 27 Aug 2024

#### **miniProxy 1.0.0 Remote File Inclusion**

miniProxy version 1.0.0 suffers from a remote file inclusion vulnerability.

- [Link](#)

—

” “Tue, 27 Aug 2024

#### **Medicine Tracker System 1.0 Insecure Settings**

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

- [Link](#)

—

” “Tue, 27 Aug 2024

***Medical Hub Directory Site 1.0 Insecure Settings***

Medical Hub Directory Site version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Tue, 27 Aug 2024

***Medical Center Portal 1.0 SQL Injection***

Medical Center Portal version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Tue, 27 Aug 2024

***Marc@TMS CMS 1.0 SQL Injection***

Marc@TMS CMS version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 27 Aug 2024

***Lodging Reservation Management System 1.0 Insecure Settings***

Lodging Reservation Management System version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Tue, 27 Aug 2024

***Login System Project 1.0 SQL Injection***

Login System Project version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Tue, 27 Aug 2024

***Loan Management System 1.0 Remote File Inclusion***

Loan Management System version 1.0 suffers from a remote file inclusion vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

***Invesalius 3.1 Remote Code Execution***

Invesalius versions 3.1.99991 through 3.1.99998 suffer from a remote code execution vulnerability.

The exploitation steps of this vulnerability involve the use of a specifically crafted DICOM file which, once imported inside the victim's client application, allows an attacker to gain remote code execution.

- [Link](#)

—

” “Mon, 26 Aug 2024

***Calibre Web 0.6.21 Cross Site Scripting***

Calibre Web version 0.6.21 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

***Helpdesk 2.0.2 Cross Site Scripting***

Helpdesk version 2.0.2 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

***SPIP 4.2.11 Code Execution***

SPIP version 4.2.11 suffers from a code execution vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

***Loan Management System 1.0 SQL Injection***

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

- [Link](#)

—

” “Mon, 26 Aug 2024

***Jobs Finder System 1.0 Cross Site Scripting***

Jobs Finder System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

***HughesNet HT2000W Satellite Modem Password Reset***

HughesNet HT2000W Satellite Modem remote password reset exploit that leverages a path traversal vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

**Human Resource Management System 2024 1.0 Cross Site Scripting**

Human Resource Management System version 2024 version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

**Employee Record Management System 1.0 SQL Injection**

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

- [Link](#)

—

” “Mon, 26 Aug 2024

**DETS Project 1.0 SQL Injection**

DETS Project version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 26 Aug 2024

**Aruba 501 CN12G5W0XX Remote Command Execution**

Aruba 501 version CN12G5W0XX suffers from a remote command execution vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

**Bang Resto 1.0 Information Disclosure**

Bang Resto version 1.0 suffers from an information disclosure vulnerability.

- [Link](#)

—

” “Mon, 26 Aug 2024

**School Log Management System 1.0 SQL Injection / Code Execution**

School Log Management System version 1.0 appears to suffers from a remote SQL injection vulnerability that allows an attacker to achieve code execution.

- [Link](#)

—

” “Mon, 26 Aug 2024

**Simple College Website 1.0 SQL Injection / Code Execution**

Simple College Website version 1.0 appears to suffers from a remote SQL injection vulnerability that allows an attacker to achieve code execution.

- [Link](#)



—

” “Fri, 23 Aug 2024

***Ray cpu\_profile Command Injection***

This Metasploit module demonstrates a command injection vulnerability in Ray via cpu\_profile.

- [Link](#)

—

”

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

“Tue, 27 Aug 2024

***ZDI-24-1182: Linux Kernel Netfilter Conntrack Type Confusion Information Disclosure Vulnerability***

- [Link](#)

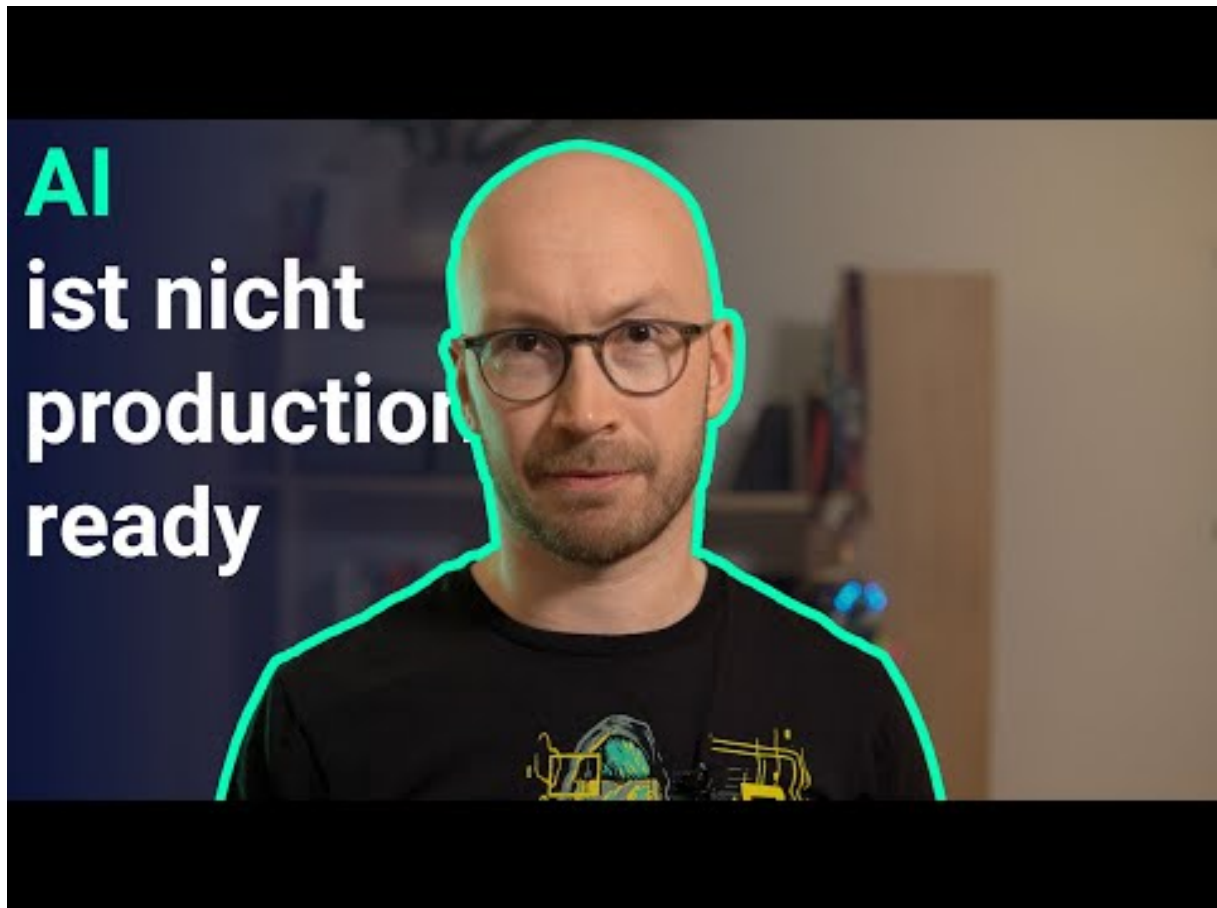
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 AI ist nicht bereit für Production (Indirekte Prompt Injection in der Slack AI)



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-08-25	Arntz Optibelt	[DEU]	<a href="#">Link</a>
2024-08-25	La Cité de la BD d'Angoulême	[FRA]	<a href="#">Link</a>
2024-08-24	Aéroport international Seattle-Tacoma	[USA]	<a href="#">Link</a>
2024-08-24	Timișoara	[ROU]	<a href="#">Link</a>
2024-08-24	Zeop	[FRA]	<a href="#">Link</a>
2024-08-21	Groupe Cirano	[REU]	<a href="#">Link</a>
2024-08-21	Halliburton	[USA]	<a href="#">Link</a>
2024-08-19	BVI Electricity Corporation (BVIEC)	[VGB]	<a href="#">Link</a>
2024-08-18	Lagoon	[NCL]	<a href="#">Link</a>
2024-08-18	Ponta Grossa	[BRA]	<a href="#">Link</a>
2024-08-18	Pittsburg	[USA]	<a href="#">Link</a>
2024-08-17	Bella Vista	[USA]	<a href="#">Link</a>
2024-08-17	Microchip Technology Incorporated	[USA]	<a href="#">Link</a>
2024-08-17	Octave	[FRA]	<a href="#">Link</a>
2024-08-16	Contarina	[ITA]	<a href="#">Link</a>
2024-08-16	Shoshone-Bannock Tribes	[USA]	<a href="#">Link</a>
2024-08-15	Canvey Infant School	[GBR]	<a href="#">Link</a>
2024-08-14	Flint	[USA]	<a href="#">Link</a>
2024-08-14	NWO (Organisation néerlandaise pour la recherche scientifique)	[NLD]	<a href="#">Link</a>
2024-08-13	District scolaire indépendant de Gadsden	[USA]	<a href="#">Link</a>
2024-08-13	IPNext	[ARG]	<a href="#">Link</a>
2024-08-12	Benson, Kearley & Associates Insurance Brokers Ltd.	[CAN]	<a href="#">Link</a>
2024-08-11	Université Paris-Saclay	[FRA]	<a href="#">Link</a>
2024-08-11	AutoCanada	[CAN]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-08-11	Itu	[BRA]	<a href="#">Link</a>
2024-08-10	2Park	[NLD]	<a href="#">Link</a>
2024-08-09	Quálitás	[MEX]	<a href="#">Link</a>
2024-08-09	Schlatter Industries AG	[CHE]	<a href="#">Link</a>
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	<a href="#">Link</a>
2024-08-08	Evolution Mining	[AUS]	<a href="#">Link</a>
2024-08-07	Killeen	[USA]	<a href="#">Link</a>
2024-08-06	Nilörn	[SWE]	<a href="#">Link</a>
2024-08-06	Sumter County Sheriff's Office	[USA]	<a href="#">Link</a>
2024-08-05	La ville de North Miami	[USA]	<a href="#">Link</a>
2024-08-05	McLaren Health Care	[USA]	<a href="#">Link</a>
2024-08-04	RMN-Grand Palais	[FRA]	<a href="#">Link</a>
2024-08-04	Regent Caravans	[AUS]	<a href="#">Link</a>
2024-08-03	Xtrim	[ECU]	<a href="#">Link</a>
2024-08-02	Ihecs	[BEL]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-27	[WT Gruber Steuerberatung GmbH]	meow	<a href="#">Link</a>
2024-08-27	[Finlogic S.p.A]	meow	<a href="#">Link</a>
2024-08-27	[Academy of Model Aeronautics]	blacksuit	<a href="#">Link</a>
2024-08-19	[Mason City Recycling Center]	qilin	<a href="#">Link</a>
2024-08-27	[Barkal Food Industries]	meow	<a href="#">Link</a>
2024-08-27	[Modulkit]	meow	<a href="#">Link</a>
2024-08-27	[Artesanía Chopo]	meow	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-27	[Crowe]	hunters	<a href="#">Link</a>
2024-08-27	[securityinstrument.com]	cactus	<a href="#">Link</a>
2024-08-26	[Microchip Technology]	play	<a href="#">Link</a>
2024-08-26	[Precom]	play	<a href="#">Link</a>
2024-08-26	[All Parks Insurance]	meow	<a href="#">Link</a>
2024-08-26	[Vans Lumber and Custom Builders]	meow	<a href="#">Link</a>
2024-08-26	[Optimize EGS]	meow	<a href="#">Link</a>
2024-08-26	[Complete Payroll Solutions]	meow	<a href="#">Link</a>
2024-08-26	[South American Tours]	meow	<a href="#">Link</a>
2024-08-26	[www.smarterp.com]	ransomhub	<a href="#">Link</a>
2024-08-26	[htsusa.com]	ransomhub	<a href="#">Link</a>
2024-08-26	[www.spie-tec.de]	ransomhub	<a href="#">Link</a>
2024-08-26	[Brookshire Dental - Hospitals & Clinics]	qilin	<a href="#">Link</a>
2024-08-16	[MacEwen Petroleum]	lynx	<a href="#">Link</a>
2024-08-26	[pocketrisk.com]	darkvault	<a href="#">Link</a>
2024-08-26	[widex.com]	blacksuit	<a href="#">Link</a>
2024-08-26	[Blue Maven Group]	monti	<a href="#">Link</a>
2024-08-26	[NewsBank]	rhysida	<a href="#">Link</a>
2024-08-26	[US Marshals Service]	hunters	<a href="#">Link</a>
2024-08-26	[onedayonly.co.za]	killsec	<a href="#">Link</a>
2024-08-26	[Affordable Tools]	rhysida	<a href="#">Link</a>
2024-08-25	[prasarana.com.my]	ransomhub	<a href="#">Link</a>
2024-08-19	[Penn Veterinary Supply INC]	qilin	<a href="#">Link</a>
2024-08-21	[Meli (BCYF & Bethany)]	qilin	<a href="#">Link</a>
2024-08-25	[dt-technologies]	qilin	<a href="#">Link</a>
2024-08-26	[autonomous.ai]	killsec	<a href="#">Link</a>
2024-08-25	[Sable International]	bianlian	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-18	[The University and College Union]	incransom	<a href="#">Link</a>
2024-08-25	[EPS Tech R&D]	handala	<a href="#">Link</a>
2024-08-24	[nwcsb.com]	blacksuit	<a href="#">Link</a>
2024-08-23	[Myelec Electrical]	lynx	<a href="#">Link</a>
2024-08-24	[www.curvc.com]	ElDorado	<a href="#">Link</a>
2024-08-24	[Eagle Safety Eyewear]	ElDorado	<a href="#">Link</a>
2024-08-18	[Wallace Construction Specialties (wcs.local)]]	lynx	<a href="#">Link</a>
2024-08-18	[Bay Sales (cog.local)]	lynx	<a href="#">Link</a>
2024-08-18	[PBS group]	lynx	<a href="#">Link</a>
2024-08-18	[Health Quality Council]	incransom	<a href="#">Link</a>
2024-08-24	[HBGJEWISHCOMMUN]	helldown	<a href="#">Link</a>
2024-08-24	[ingotbrokers.com]	darkvault	<a href="#">Link</a>
2024-08-24	[Hofmann Malerei AG]	cicada3301	<a href="#">Link</a>
2024-08-24	[Studio Legale Associato Isolabella]	bianlian	<a href="#">Link</a>
2024-08-22	[HL Lawson & Sons]	incransom	<a href="#">Link</a>
2024-08-23	[terralogs.com.br]	killsec	<a href="#">Link</a>
2024-08-23	[Chama Gaucha]	cicada3301	<a href="#">Link</a>
2024-08-23	[idahopacific.com]	abyss	<a href="#">Link</a>
2024-08-23	[barryavenueplating]	helldown	<a href="#">Link</a>
2024-08-23	[rsk-immobilien]	helldown	<a href="#">Link</a>
2024-08-23	[Crimson Interactive]	hunters	<a href="#">Link</a>
2024-08-23	[www.seaeng.com]	dAn0n	<a href="#">Link</a>
2024-08-23	[Stjamesplace.org]	cloak	<a href="#">Link</a>
2024-08-23	[Saeilo]	metaencryptor	<a href="#">Link</a>
2024-08-22	[schoolrush.com]	killsec	<a href="#">Link</a>
2024-08-22	[Life University]	metaencryptor	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-22	[Sherwood Stainless & Aluminium]	dragonforce	<a href="#">Link</a>
2024-08-22	[Igloo Cellulose]	dragonforce	<a href="#">Link</a>
2024-08-22	[Raifalsa-Alelor]	dragonforce	<a href="#">Link</a>
2024-08-22	[Deane Roofing and Cladding]	dragonforce	<a href="#">Link</a>
2024-08-22	[instadriver.co]	killsec	<a href="#">Link</a>
2024-08-22	[cincinnatipainphysicians]	helldown	<a href="#">Link</a>
2024-08-22	[Don't Waste Group]	incransom	<a href="#">Link</a>
2024-08-22	[Kronick Moskovitz Tiedemann & Girard]	rhysida	<a href="#">Link</a>
2024-08-22	[UFCW Local 135]	cicada3301	<a href="#">Link</a>
2024-08-22	[EBA Ernest Bland Associates]	cicada3301	<a href="#">Link</a>
2024-08-22	[level.game]	killsec	<a href="#">Link</a>
2024-08-22	[antaeustravel.com]	blackout	<a href="#">Link</a>
2024-08-22	[rylandpeters.com]	apt73	<a href="#">Link</a>
2024-08-22	[saudi arabia(general secretariat of the military service council)]	ransomhub	<a href="#">Link</a>
2024-08-22	[Engedi]	rhysida	<a href="#">Link</a>
2024-08-22	[EPS Tech confidential source code ( military )]	handala	<a href="#">Link</a>
2024-08-16	[policiaauxiliarcusaem.com.mx]	lockbit3	<a href="#">Link</a>
2024-08-14	[Larc]	incransom	<a href="#">Link</a>
2024-08-22	[kbosecurity.co.uk]	helldown	<a href="#">Link</a>
2024-08-22	[khonaysser.com]	helldown	<a href="#">Link</a>
2024-08-21	[beinlaw.co.il - Prof. Bein & Co.]	BrainCipher	<a href="#">Link</a>
2024-08-21	[The SMS Group]	play	<a href="#">Link</a>
2024-08-21	[Grid Subject Matter Experts]	play	<a href="#">Link</a>
2024-08-21	[Quilvest Capital Partners]	play	<a href="#">Link</a>
2024-08-21	[Armour Coatings]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-21	[RCG]	play	<a href="#">Link</a>
2024-08-21	[Policy Administration Solutions]	play	<a href="#">Link</a>
2024-08-21	[Dunlop Aircraft Tyres]	cloak	<a href="#">Link</a>
2024-08-21	[Vibo.dk]	cloak	<a href="#">Link</a>
2024-08-21	[Hvb-ingenieure.de]	cloak	<a href="#">Link</a>
2024-08-21	[Westermans.com]	cloak	<a href="#">Link</a>
2024-08-21	[Jinny Corporation]	akira	<a href="#">Link</a>
2024-08-21	[BARRYAVEPLATING]	helldown	<a href="#">Link</a>
2024-08-21	[RSK-IMMOBILIEN]	helldown	<a href="#">Link</a>
2024-08-20	[capitalfund1.com]	ransomhub	<a href="#">Link</a>
2024-08-21	[www.pindrophearing.co.uk]	apt73	<a href="#">Link</a>
2024-08-21	[www.banhampoultry.co.uk]	ransomhub	<a href="#">Link</a>
2024-08-21	[kidkraft.com]	lynx	<a href="#">Link</a>
2024-08-21	[Luigi Convertini]	ciphbit	<a href="#">Link</a>
2024-08-21	[Findel]	cicada3301	<a href="#">Link</a>
2024-08-21	[HOERBIGER Holding]	akira	<a href="#">Link</a>
2024-08-21	[Olympus Financial]	rhysida	<a href="#">Link</a>
2024-08-21	[spvmhc.org]	abyss	<a href="#">Link</a>
2024-08-21	[Burns Industrial Equipment]	meow	<a href="#">Link</a>
2024-08-21	[globacap.com]	apt73	<a href="#">Link</a>
2024-08-20	[Codival]	spacebears	<a href="#">Link</a>
2024-08-21	[jpoint.in]	killsec	<a href="#">Link</a>
2024-08-20	[inlighten.net]	ransomhub	<a href="#">Link</a>
2024-08-20	[blowerdempsey.com]	ransomhub	<a href="#">Link</a>
2024-08-20	[ATP]	helldown	<a href="#">Link</a>
2024-08-20	[Rushlift (lks.net)]	lynx	<a href="#">Link</a>
2024-08-20	[North Georgia Brick]	akira	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-20	[Akkanat Holding]	hunters	<a href="#">Link</a>
2024-08-19	[Percento Technologies Internationa]	medusa	<a href="#">Link</a>
2024-08-19	[OSG.COM]	ransomhub	<a href="#">Link</a>
2024-08-14	[imobesidade.com.br]	ransomhub	<a href="#">Link</a>
2024-08-19	[Waynesboro Nurseries]	rhysida	<a href="#">Link</a>
2024-08-19	[The Transit Authority of Northern Kentucky (TANK)]	akira	<a href="#">Link</a>
2024-08-19	[Khonaysser]	helldown	<a href="#">Link</a>
2024-08-11	[Jangho Group]	ransomhouse	<a href="#">Link</a>
2024-08-19	[Certified Transmission]	meow	<a href="#">Link</a>
2024-08-19	[Bandier]	blacksuit	<a href="#">Link</a>
2024-08-18	[ccsdschools.com]	ransomhub	<a href="#">Link</a>
2024-08-19	[Ferraro Group]	hunters	<a href="#">Link</a>
2024-08-18	[kbo]	helldown	<a href="#">Link</a>
2024-08-18	[Mohawk Valley Cardiology PC]	bianlian	<a href="#">Link</a>
2024-08-18	[PBC Companies]	bianlian	<a href="#">Link</a>
2024-08-17	[Yang Enterprises]	dragonforce	<a href="#">Link</a>
2024-08-17	[Carver Companies]	dragonforce	<a href="#">Link</a>
2024-08-17	[J&J Network Engineering]	dragonforce	<a href="#">Link</a>
2024-08-18	[PER4MANCE]	dragonforce	<a href="#">Link</a>
2024-08-18	[SMK Ingenieurbüro]	dragonforce	<a href="#">Link</a>
2024-08-18	[Cosmetic Dental Group]	trinity	<a href="#">Link</a>
2024-08-17	[TELECO]	stormous	<a href="#">Link</a>
2024-08-17	[peoplewell.com]	darkvault	<a href="#">Link</a>
2024-08-17	[aerworldwide.com]	lockbit3	<a href="#">Link</a>
2024-08-17	[awsag.com]	madliberator	<a href="#">Link</a>
2024-08-17	[www.albynhousing.org.uk]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-17	[www.lennartsfors.com]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.allanmcneill.co.nz]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.martinswood.herts.sch.uk]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.gmchc.org]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.regentcaravans.com.au]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.netconfig.co.za]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.manotherm.ie]	ransomhub	<a href="#">Link</a>
2024-08-17	[tiendasmacuto.com]	BrainCipher	<a href="#">Link</a>
2024-08-15	[nrcollecties.nl]	ransomhub	<a href="#">Link</a>
2024-08-17	[zyxel]	helldown	<a href="#">Link</a>
2024-08-10	[www.wmwmeyer.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[www.vinakom.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[Keios Development Consulting]	ciphbit	<a href="#">Link</a>
2024-08-16	[Lennartsfors AB]	meow	<a href="#">Link</a>
2024-08-16	[Rostance Edwards]	meow	<a href="#">Link</a>
2024-08-16	[SuperDrob S.A.]	hunters	<a href="#">Link</a>
2024-08-16	[Sterling Rope]	rhysida	<a href="#">Link</a>
2024-08-16	[www.patelco.org]	ransomhub	<a href="#">Link</a>
2024-08-14	[ljglaw.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[Hiesmayr Haustechnik]	qilin	<a href="#">Link</a>
2024-08-15	[www.aaconsultinc.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[promises2kids.org]	qilin	<a href="#">Link</a>
2024-08-16	[BTS Biogas]	hunters	<a href="#">Link</a>
2024-08-15	[www.isnart.it]	ransomhub	<a href="#">Link</a>
2024-08-15	[www.atwoodcherny.com]	ransomhub	<a href="#">Link</a>
2024-08-13	[Mill Creek Lumber]	play	<a href="#">Link</a>
2024-08-14	[Patterson Health Center]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-15	[www.prinsotel.com]	qilin	<a href="#">Link</a>
2024-08-15	[Seaway Manufacturing Corp.]	fog	<a href="#">Link</a>
2024-08-15	[FD S.R.L.]	ciphbit	<a href="#">Link</a>
2024-08-15	[The Pyle Group]	medusa	<a href="#">Link</a>
2024-08-15	[Zydus Pharmaceuticals]	meow	<a href="#">Link</a>
2024-08-15	[EPS Tech Ltd]	handala	<a href="#">Link</a>
2024-08-15	[MBS Radio]	metaencryptor	<a href="#">Link</a>
2024-08-15	[Liberty Resources]	rhysida	<a href="#">Link</a>
2024-08-15	[megatravel.com.mx]	darkvault	<a href="#">Link</a>
2024-08-14	[startaxi.com]	killsec	<a href="#">Link</a>
2024-08-14	[Boni]	akira	<a href="#">Link</a>
2024-08-14	[The Washington Times]	rhysida	<a href="#">Link</a>
2024-08-12	[Benson Kearley IFG - Insurance Brokers & Financial Advisors]	bianlian	<a href="#">Link</a>
2024-08-14	[Texas Centers for Infectious Disease Associates]	bianlian	<a href="#">Link</a>
2024-08-14	[Thompson Davis & Co]	bianlian	<a href="#">Link</a>
2024-08-14	[police.praca.gov.pl]	ransomhub	<a href="#">Link</a>
2024-08-14	[mmtransport.com]	dAn0n	<a href="#">Link</a>
2024-08-14	[Riley Pope & Laney]	cicada3301	<a href="#">Link</a>
2024-08-13	[hugwi]	helldown	<a href="#">Link</a>
2024-08-13	[Forrec]	blacksuit	<a href="#">Link</a>
2024-08-13	[American Contract Systems]	meow	<a href="#">Link</a>
2024-08-13	[Element Food Solutions]	meow	<a href="#">Link</a>
2024-08-13	[Aerotech Solutions]	meow	<a href="#">Link</a>
2024-08-13	[E-Z UP]	meow	<a href="#">Link</a>
2024-08-13	[Safefood]	meow	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-13	[Gaston Fence]	meow	<a href="#">Link</a>
2024-08-13	[Parker Development Company]	play	<a href="#">Link</a>
2024-08-13	[Air International Thermal Systems]	play	<a href="#">Link</a>
2024-08-13	[Adina Design]	play	<a href="#">Link</a>
2024-08-13	[CinemaTech]	play	<a href="#">Link</a>
2024-08-13	[Erie Meats]	play	<a href="#">Link</a>
2024-08-13	[M??? ???k ??????]	play	<a href="#">Link</a>
2024-08-13	[SCHLATTNER]	helldown	<a href="#">Link</a>
2024-08-13	[deganis]	helldown	<a href="#">Link</a>
2024-08-13	[The White Center Community Development Association]	rhysida	<a href="#">Link</a>
2024-08-13	[lenmed.co.za]	darkvault	<a href="#">Link</a>
2024-08-13	[gpf.org.za]	darkvault	<a href="#">Link</a>
2024-08-13	[Banner and Associates]	trinity	<a href="#">Link</a>
2024-08-13	[Southwest Family Medicine Associates]	bianlian	<a href="#">Link</a>
2024-08-13	[glazkov.co.il]	darkvault	<a href="#">Link</a>
2024-08-05	[XPERT Business Solutions GmbH]	helldown	<a href="#">Link</a>
2024-08-05	[MyFreightWorld]	helldown	<a href="#">Link</a>
2024-08-09	[cbmm]	helldown	<a href="#">Link</a>
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	<a href="#">Link</a>
2024-08-11	[briju]	helldown	<a href="#">Link</a>
2024-08-11	[vindix]	helldown	<a href="#">Link</a>
2024-08-11	[Albatros]	helldown	<a href="#">Link</a>
2024-08-12	[NetOne]	hunters	<a href="#">Link</a>
2024-08-12	[fabamaq.com]	BrainCipher	<a href="#">Link</a>
2024-08-12	[cyceron.fr]	BrainCipher	<a href="#">Link</a>
2024-08-12	[bedford.k12.oh.us]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-12	[Warwick Hotels and Resorts]	lynx	<a href="#">Link</a>
2024-08-12	[VVS-Experten]	cicada3301	<a href="#">Link</a>
2024-08-12	[Brookshire Dental]	qilin	<a href="#">Link</a>
2024-08-07	[Alvan Blanch Development]	lynx	<a href="#">Link</a>
2024-08-11	[parkerdevco.com]	dispossessor	<a href="#">Link</a>
2024-08-11	[naturalcuriosities.com]	ransomhub	<a href="#">Link</a>
2024-08-11	[TelPro]	play	<a href="#">Link</a>
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	<a href="#">Link</a>
2024-08-11	[Amco Metal Industrial Corporation]	qilin	<a href="#">Link</a>
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	<a href="#">Link</a>
2024-08-11	[Moser Wealth Advisors]	rhysida	<a href="#">Link</a>
2024-08-09	[alliuminteriors.co.nz]	ransomhub	<a href="#">Link</a>
2024-08-11	[robertshvac.com]	abyss	<a href="#">Link</a>
2024-08-11	[dmmerch.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[luisoliveras.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[legacypas.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[allweatheraa.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[soprema.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[exol-lubricants.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[fremontschools.net]	lockbit3	<a href="#">Link</a>
2024-08-11	[acdexpress.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[clinatezza.com.pe]	lockbit3	<a href="#">Link</a>
2024-08-11	[divaris.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[sullivansteelservice.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[johnllowery.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[qespavements.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[emanic.net]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-11	[Hanon Systems]	hunters	<a href="#">Link</a>
2024-08-10	[kronospublic.com]	lockbit3	<a href="#">Link</a>
2024-08-10	[Brontoo Technology Solutions]	ransomexx	<a href="#">Link</a>
2024-08-07	[Cydcor]	dragonforce	<a href="#">Link</a>
2024-08-09	[Credible Group]	play	<a href="#">Link</a>
2024-08-09	[Nilorngruppen AB]	play	<a href="#">Link</a>
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	<a href="#">Link</a>
2024-08-09	[Anniversary Holding Company]	bianlian	<a href="#">Link</a>
2024-08-09	[GCA Global Cargo Alliance]	bianlian	<a href="#">Link</a>
2024-08-09	[Majestic Metals]	bianlian	<a href="#">Link</a>
2024-08-09	[dhcgrp.com]	ransomhub	<a href="#">Link</a>
2024-08-05	[Boombah Inc.]	incransom	<a href="#">Link</a>
2024-08-09	[www.dunnsolutions.com]	dAn0n	<a href="#">Link</a>
2024-08-09	[Sumter County Sheriff]	rhysida	<a href="#">Link</a>
2024-08-06	[pierrediamonds.com.au]	ransomhub	<a href="#">Link</a>
2024-08-08	[golfoy.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[inv-dar.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[icarasia.com]	killsec	<a href="#">Link</a>
2024-08-08	[rationalenterprise.com]	ransomhub	<a href="#">Link</a>
2024-08-02	[modernceramics.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	<a href="#">Link</a>
2024-08-08	[tibaitservices.com]	cactus	<a href="#">Link</a>
2024-08-08	[mihlfeld.com]	cactus	<a href="#">Link</a>
2024-08-08	[Horizon View Medical Center]	everest	<a href="#">Link</a>
2024-08-08	[comoferta.com]	darkvault	<a href="#">Link</a>
2024-08-08	[NIDEC CORPORATION]	everest	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-08	[mercadomineiro.com.br]	darkvault	<a href="#">Link</a>
2024-08-07	[hudsoncivil.com.au]	ransomhub	<a href="#">Link</a>
2024-08-07	[www.jgsummit.com.ph]	ransomhub	<a href="#">Link</a>
2024-08-07	[Bayhealth Hospital]	rhysida	<a href="#">Link</a>
2024-08-07	[amplicon.com]	ransomhub	<a href="#">Link</a>
2024-08-06	[infotexim.pe]	ransomhub	<a href="#">Link</a>
2024-08-07	[suandco.com]	madliberator	<a href="#">Link</a>
2024-08-07	[Anderson Oil & Gas]	hunters	<a href="#">Link</a>
2024-08-07	[bonatra.com]	killsec	<a href="#">Link</a>
2024-08-07	[FatBoy Cellular]	meow	<a href="#">Link</a>
2024-08-07	[KLA]	meow	<a href="#">Link</a>
2024-08-07	[HUD User]	meow	<a href="#">Link</a>
2024-08-06	[msprocuradores.es]	madliberator	<a href="#">Link</a>
2024-08-06	[www.carri.com]	alphalocker	<a href="#">Link</a>
2024-08-06	[www.consorzioinnova.it]	alphalocker	<a href="#">Link</a>
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	<a href="#">Link</a>
2024-08-06	[biw-burger.de]	alphalocker	<a href="#">Link</a>
2024-08-06	[www.sobha.com]	ransomhub	<a href="#">Link</a>
2024-08-06	[Alternate Energy]	play	<a href="#">Link</a>
2024-08-06	[True Blue Environmental]	play	<a href="#">Link</a>
2024-08-06	[Granit Design]	play	<a href="#">Link</a>
2024-08-06	[KinetX]	play	<a href="#">Link</a>
2024-08-06	[Omni Family Health]	hunters	<a href="#">Link</a>
2024-08-06	[IOI Corporation Berhad]	fog	<a href="#">Link</a>
2024-08-06	[Ziba Design]	fog	<a href="#">Link</a>
2024-08-06	[Casco Antiguo]	hunters	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-06	[Fractalia Group]	hunters	<a href="#">Link</a>
2024-08-06	[Banx Systems]	meow	<a href="#">Link</a>
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>
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	<a href="#">Link</a>
2024-08-02	[retaildata LLC.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>



Datum	Opfer	Ransomware-Gruppe	Webseite
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.