

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241023



## 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 . . . . .	18
<b>5 Die Hacks der Woche</b>	<b>19</b>
5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor) . . . . .	19
<b>6 Cyberangriffe: (Okt)</b>	<b>20</b>
<b>7 Ransomware-Erpressungen: (Okt)</b>	<b>21</b>
<b>8 Quellen</b>	<b>34</b>
8.1 Quellenverzeichnis . . . . .	34
<b>9 Impressum</b>	<b>35</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

**FortiManager: Update dichtet offenbar attackiertes Sicherheitsleck ab**

Ohne öffentliche Informationen hat Fortinet Updates für FortiManager veröffentlicht. Sie schließen offenbar attackierte Sicherheitslücken.

- [Link](#)

---

**Roundcube Webmail: Angriffe mit gefälschten Anhängen**

IT-Sicherheitsforscher haben Angriffe auf eine Stored-Cross-Site-Scripting-Lücke in Roundcube Webmail beobachtet. Ein Update ist verfügbar.

- [Link](#)

---

**Sicherheitsupdates: DoS-Attacken auf IBM-Software möglich**

IBMs Entwickler haben Schwachstellen in App Connect Enterprise und WebSphere Application Server geschlossen.

- [Link](#)

---

**Atlassian: Schwachstellen machen Bitbucket, Confluence und Jira verwundbar**

In Bitbucket, Confluence und Jira lauern Sicherheitslücken, die etwa Informationsabfluss oder Denial-of-Service ermöglichen.

- [Link](#)

---

**Ubiquiti Unifi Network Server: Hochriskantes Leck ermöglicht Rechteausweitung**

In Ubiquitis Unifi Network Server klafft eine hochriskante Schwachstelle. Angreifer können dadurch ihre Rechte ausweiten.

- [Link](#)

---

**Spring Framework: Angreifer können Dateien einsehen**

Updates schließen Schwachstellen in Spring Framework. Für einige Versionen ist der Support ausgelaufen und Patches gibt es nicht mehr für alle Nutzer.

- [Link](#)

---

**Sicherheitsupdates: Angreifer können über Grafana-Lücke eigene Befehle ausführen**

Das Datenvisualisierungswerkzeug Grafana ist verwundbar, und Angreifer können auf Systemen eigene Befehle ausführen und unter anderem Passwörter einsehen.

- [Link](#)

---

---

***Angreifer können PCs mit Virenschutz von Bitdefender und Trend Micro attackieren***

Sicherheitsupdates schließen Schwachstellen in Bitdefender Total Security und Trend Micro Deep Security Agent.

- [Link](#)

---

***Kritische Sicherheitslücke: Angreifer können Kubernetes als Root attackieren***

Bestimmte Kubernetes Image Builder erzeugen VM-Images mit statischen Zugangsdaten. Admins müssen bestehende Images neu erstellen.

- [Link](#)

---

***Oracle schützt Softwareprodukte mit 334 Sicherheitsupdates***

Mit seinen quartalsweise erscheinenden Sicherheitsupdates sichert Oracle abermals das eigene Softwareportfolio ab.

- [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	0.957580000	0.994930000	<a href="#">Link</a>
CVE-2023-6895	0.925010000	0.990740000	<a href="#">Link</a>
CVE-2023-6553	0.945310000	0.992970000	<a href="#">Link</a>
CVE-2023-6019	0.933700000	0.991610000	<a href="#">Link</a>
CVE-2023-6018	0.911590000	0.989670000	<a href="#">Link</a>
CVE-2023-52251	0.948240000	0.993390000	<a href="#">Link</a>
CVE-2023-4966	0.971220000	0.998360000	<a href="#">Link</a>
CVE-2023-49103	0.949290000	0.993540000	<a href="#">Link</a>
CVE-2023-48795	0.965360000	0.996530000	<a href="#">Link</a>
CVE-2023-47246	0.960640000	0.995430000	<a href="#">Link</a>
CVE-2023-46805	0.961520000	0.995590000	<a href="#">Link</a>
CVE-2023-46747	0.972980000	0.998980000	<a href="#">Link</a>
CVE-2023-46604	0.970640000	0.998130000	<a href="#">Link</a>
CVE-2023-4542	0.941060000	0.992430000	<a href="#">Link</a>
CVE-2023-43208	0.974590000	0.999680000	<a href="#">Link</a>
CVE-2023-43177	0.954040000	0.994330000	<a href="#">Link</a>
CVE-2023-42793	0.970480000	0.998080000	<a href="#">Link</a>
CVE-2023-41892	0.905460000	0.989220000	<a href="#">Link</a>
CVE-2023-41265	0.920970000	0.990320000	<a href="#">Link</a>
CVE-2023-39143	0.905600000	0.989230000	<a href="#">Link</a>
CVE-2023-38205	0.954790000	0.994440000	<a href="#">Link</a>
CVE-2023-38203	0.964750000	0.996320000	<a href="#">Link</a>
CVE-2023-38146	0.920950000	0.990320000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-38035	0.974710000	0.999750000	<a href="#">Link</a>
CVE-2023-36845	0.967920000	0.997250000	<a href="#">Link</a>
CVE-2023-3519	0.964810000	0.996340000	<a href="#">Link</a>
CVE-2023-35082	0.967900000	0.997240000	<a href="#">Link</a>
CVE-2023-35078	0.967840000	0.997200000	<a href="#">Link</a>
CVE-2023-34993	0.973050000	0.999010000	<a href="#">Link</a>
CVE-2023-34634	0.923140000	0.990510000	<a href="#">Link</a>
CVE-2023-34362	0.970450000	0.998070000	<a href="#">Link</a>
CVE-2023-34105	0.927500000	0.990960000	<a href="#">Link</a>
CVE-2023-34039	0.941110000	0.992450000	<a href="#">Link</a>
CVE-2023-3368	0.937940000	0.992070000	<a href="#">Link</a>
CVE-2023-33246	0.971590000	0.998460000	<a href="#">Link</a>
CVE-2023-32315	0.973230000	0.999100000	<a href="#">Link</a>
CVE-2023-30625	0.953820000	0.994300000	<a href="#">Link</a>
CVE-2023-30013	0.962230000	0.995740000	<a href="#">Link</a>
CVE-2023-29300	0.967820000	0.997200000	<a href="#">Link</a>
CVE-2023-29298	0.969430000	0.997660000	<a href="#">Link</a>
CVE-2023-28432	0.921730000	0.990400000	<a href="#">Link</a>
CVE-2023-28343	0.957970000	0.994990000	<a href="#">Link</a>
CVE-2023-28121	0.929610000	0.991180000	<a href="#">Link</a>
CVE-2023-27524	0.969670000	0.997750000	<a href="#">Link</a>
CVE-2023-27372	0.973760000	0.999300000	<a href="#">Link</a>
CVE-2023-27350	0.968980000	0.997520000	<a href="#">Link</a>
CVE-2023-26469	0.955890000	0.994640000	<a href="#">Link</a>
CVE-2023-26360	0.963280000	0.995960000	<a href="#">Link</a>
CVE-2023-26035	0.967750000	0.997170000	<a href="#">Link</a>
CVE-2023-25717	0.950620000	0.993720000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.966130000	0.996720000	<a href="#">Link</a>
CVE-2023-2479	0.961840000	0.995670000	<a href="#">Link</a>
CVE-2023-24489	0.972860000	0.998920000	<a href="#">Link</a>
CVE-2023-23752	0.949000000	0.993480000	<a href="#">Link</a>
CVE-2023-23333	0.960430000	0.995360000	<a href="#">Link</a>
CVE-2023-22527	0.970410000	0.998040000	<a href="#">Link</a>
CVE-2023-22518	0.962690000	0.995820000	<a href="#">Link</a>
CVE-2023-22515	0.973650000	0.999250000	<a href="#">Link</a>
CVE-2023-21839	0.941470000	0.992480000	<a href="#">Link</a>
CVE-2023-21554	0.952650000	0.994100000	<a href="#">Link</a>
CVE-2023-20887	0.971130000	0.998320000	<a href="#">Link</a>
CVE-2023-1698	0.923310000	0.990550000	<a href="#">Link</a>
CVE-2023-1671	0.962220000	0.995730000	<a href="#">Link</a>
CVE-2023-0669	0.971830000	0.998530000	<a href="#">Link</a>

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

Tue, 22 Oct 2024

#### **[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Tue, 22 Oct 2024

#### **[UPDATE] [hoch] Roundcube: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Roundcube ausnutzen, um beliebige Kommandos auszuführen oder einen Cross-Site Scripting (XSS) Angriff durchzuführen.

- [Link](#)

—



Tue, 22 Oct 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Roundcube ausnutzen, um einen Cross-Site Scripting Angriff zu starten oder beliebigen Code auszuführen.

- [Link](#)

—

Tue, 22 Oct 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](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Tue, 22 Oct 2024

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

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer 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](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Tue, 22 Oct 2024

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

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

- [Link](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] VMware vCenter Server: Mehrere Schwachstellen ermöglichen Codeausführung und Privilegienerweiterung**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in VMware vCenter Server und VMware Cloud Foundation ausnutzen, um beliebigen Programmcode auszuführen und erweiterte Rechte zu erlangen.

- [Link](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- [Link](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] GNOME: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein lokaler Angreifer kann mehrere Schwachstellen in GNOME ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Tue, 22 Oct 2024

**[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Denial of Service und Remote-Code-Ausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder um beliebigen Code auszuführen.

- [Link](#)

—

Mon, 21 Oct 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

Mon, 21 Oct 2024

**[UPDATE] [kritisch] PHP: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Informationen preiszugeben und andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Mon, 21 Oct 2024

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

Ein Angreifer kann mehrere Schwachstellen in Redis ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code auszuführen.

- [Link](#)

—

Mon, 21 Oct 2024

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Mon, 21 Oct 2024

**[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Schwachstelle ermöglicht Code-ausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Mozilla Firefox, Firefox ESR und Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Mon, 21 Oct 2024

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

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

- [Link](#)

—

Fri, 18 Oct 2024

**[NEU] [hoch] Bitdefender Total Security: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen**

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Bitdefender Total Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/22/2024	[Debian dsa-5795 : python3-sql - security update]	critical
10/22/2024	[LangChain < 0.2.4 RCE]	critical
10/22/2024	[Ollama < 0.3.13 RCE]	critical
10/22/2024	[Debian dla-3932 : python3-sql - security update]	critical
10/21/2024	[Adobe Reader < 15.006.30172 / 15.016.20039 Multiple Vulnerabilities (APSB16-14) (macOS)]	critical
10/21/2024	[Adobe FrameMaker Publishing Server 2022 < 17.0.1 (2022.0.1) Security Feature Bypass (APSB23-58)]	critical
10/21/2024	[Adobe Digital Editions < 4.5.9 Multiple Vulnerabilities (APSB18-27) (macOS)]	critical
10/21/2024	[Adobe Reader < 15.006.30198 / 15.017.20050 Multiple Vulnerabilities (APSB16-26) (macOS)]	critical
10/21/2024	[Adobe Digital Editions < 3.0 (APSB14-03) (macOS)]	critical
10/22/2024	[RHEL 6 : odh-operator-container (Unpatched Vulnerability)]	high

Datum	Schwachstelle	Bewertung
10/22/2024	[Ubuntu 22.04 LTS : Linux kernel (GKE) vulnerabilities (USN-7072-2)]	high
10/22/2024	[Ubuntu 20.04 LTS : Firefox vulnerability (USN-7078-1)]	high
10/22/2024	[RHEL 9 : NetworkManager-libreswan (RHSA-2024:8312)]	high
10/22/2024	[Google Chrome < 130.0.6723.69 Multiple Vulnerabilities]	high
10/22/2024	[Google Chrome < 130.0.6723.69 Multiple Vulnerabilities]	high
10/22/2024	[Google Chrome < 130.0.6723.70 Multiple Vulnerabilities]	high
10/22/2024	[RHEL 7 : NetworkManager-libreswan (RHSA-2024:8338)]	high
10/21/2024	[Adobe Reader < 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-15) (macOS)]	high
10/21/2024	[Adobe Animate 20.x < 20.0.0 A Vulnerability (APSB19-34)]	high
10/21/2024	[Adobe Illustrator < 25.4.7 / 26.0.0 < 26.4.0 Multiple Vulnerabilities (APSB22-41) (macOS)]	high
10/21/2024	[Adobe InDesign 15.0.0 < 15.1.2 Multiple Arbitrary Code Execution (APSB20-52) (macOS)]	high
10/21/2024	[Adobe Illustrator < 25.2.3 Multiple Arbitrary code execution (APSB21-24) (macOS)]	high
10/21/2024	[Adobe Bridge 10.x < 10.0 Multiple Vulnerabilities (APSB19-53)]	high
10/21/2024	[Adobe Creative Cloud < 3.7.0.272 Multiple Vulnerabilities (APSB16-21)]	high
10/21/2024	[Adobe After Effects < 18.4.6 / 22.0.0 < 22.3.0 Multiple Arbitrary code execution (APSB22-19) (macOS)]	high
10/21/2024	[Adobe After Effects < 18.2 Multiple Vulnerabilities (APSB21-33) (macOS)]	high
10/21/2024	[Adobe Media Encoder < 14.3 Multiple Vulnerabilities (APSB20-36) (macOS)]	high
10/21/2024	[Adobe Illustrator < 25.0 Multiple Vulnerabilities (APSB20-53) (macOS)]	high

Datum	Schwachstelle	Bewertung
10/21/2024	[Adobe Creative Cloud < 4.0.0.185 Multiple Vulnerabilities (APSB17-13)]	high
10/21/2024	[Adobe Animate 20.x < 20.0.0 A Vulnerability (APSB19-34)]	high
10/21/2024	[Adobe Creative Cloud < 3.8.0.310 (APSB16-34)]	high
10/21/2024	[Adobe Bridge 10.x < 10.0 Multiple Vulnerabilities (APSB19-53)]	high
10/21/2024	[Slackware Linux 15.0 openssl Vulnerability (SSA:2024-295-01)]	high
10/21/2024	[Rockwell (CVE-2024-6207)]	high
10/21/2024	[Siemens CP 343-1 Devices Improper Verification of Source of a Communication Channel (CVE-2023-51440)]	high
10/21/2024	[Cisco NX-OS Protection Mechanism Failure (CVE-2024-20284)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Tue, 22 Oct 2024

#### **ABB Cylon Aspect 3.08.01 persistenceManagerAjax.php Command Injection**

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the directory HTTP POST parameter called by the persistenceManagerAjax.php script.

- [Link](#)

—

” “Tue, 22 Oct 2024

#### **Linux Dangling PFN Mapping / Use-After-Free**

An error path in usbdev\_mmap() (where remap\_pfn\_range() fails midway through) frees pages before the PFN mapping pointing to those pages is cleaned up, making physical page use-after-free possible. Some other drivers look like they might have similar issues.

- [Link](#)

—

” “Mon, 21 Oct 2024

***Rittal IoT Interface / CMC III Processing Unit Signature Verification / Session ID***

Rittal IoT Interface and CMC III Processing Unit versions prior to 6.21.00.2 suffer from improper signature verification and predictable session identifier vulnerabilities.

- [Link](#)

—

” “Fri, 18 Oct 2024

***Magento / Adobe Commerce Remote Code Execution***

This Metasploit module uses a combination of an arbitrary file read (CVE-2024-34102) and a buffer overflow in glibc (CVE-2024-2961). It allows for unauthenticated remote code execution on various versions of Magento and Adobe Commerce (and earlier versions if the PHP and glibc versions are also vulnerable). Versions affected include 2.4.7 and earlier, 2.4.6-p5 and earlier, 2.4.5-p7 and earlier, and 2.4.4-p8 and earlier.

- [Link](#)

—

” “Fri, 18 Oct 2024

***ABB Cylon Aspect 3.08.01 databaseFileDelete.php Command Injection***

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the file HTTP POST parameter called by the databaseFileDelete.php script.

- [Link](#)

—

” “Fri, 18 Oct 2024

***IBM Security Verify Access 10.0.8 Open Redirection***

IBM Security Verify Access versions 10.0.0 through 10.0.8 suffer from an OAUTH related open redirection vulnerability.

- [Link](#)

—

” “Thu, 17 Oct 2024

***ABB Cylon Aspect 3.08.01 networkDiagAjax.php Remote Network Utility Execution***

ABB Cylon Aspect version 3.08.01 allows an unauthenticated attacker to perform network operations such as ping, traceroute, or nslookup on arbitrary hosts or IPs by sending a crafted GET request to networkDiagAjax.php. This could be exploited to interact with or probe internal or external systems, leading to internal information disclosure and misuse of network resources.

- [Link](#)

—

” “Thu, 17 Oct 2024

***SofaWiki 3.9.2 Cross Site Scripting***

SofaWiki version 3.9.2 suffers from a reflective cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 17 Oct 2024

***SofaWiki 3.9.2 Cross Site Scripting***

SofaWiki version 3.9.2 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 17 Oct 2024

***SofaWiki 3.9.2 Shell Upload***

SofaWiki version 3.9.2 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Wed, 16 Oct 2024

***BYOB Unauthenticated Remote Code Execution***

This Metasploit module exploits two vulnerabilities in the BYOB (Build Your Own Botnet) web GUI. It leverages an unauthenticated arbitrary file write that allows modification of the SQLite database, adding a new admin user. It also uses an authenticated command injection in the payload generation page. These vulnerabilities remain unpatched.

- [Link](#)

—

” “Wed, 16 Oct 2024

***ABB Cylon Aspect 3.08.01 mapConfigurationDownload.php Configuration Download***

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated configuration download vulnerability. This can be exploited to download the SQLite DB that contains the configuration mappings information via the FTControlServlet by directly calling the mapConfigurationDownload.php script.

- [Link](#)

—

” “Tue, 15 Oct 2024

***ABB Cylon Aspect 3.08.00 sslCertAjax.php Remote Command Execution***

ABB Cylon Aspect version 3.08.00 suffers from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the country, state, locality, organization, and hostname HTTP POST parameters called by the sslCertAjax.php script.

- [Link](#)

—

” “Tue, 15 Oct 2024

***Dolibarr 20.0.1 SQL Injection***

Dolibarr version 20.0.1 suffers from a remote SQL injection vulnerability.



- [Link](#)

—

” “Tue, 15 Oct 2024

***WatchGuard XTM Firebox 12.5.x Buffer Overflow***

WatchGuard XTM Firebox version 12.5.x suffers from a buffer overflow vulnerability.

- [Link](#)

—

” “Tue, 15 Oct 2024

***msm 5.15 Arbitrary Kernel Address Access***

This bug was found in msm-5.15 using tag KERNEL.PLATFORM.2.1.r1-05400-kernel.0. The fastrpc\_file struct contains a flag, is\_compat, that is set if the 32-bit compat\_ioctl vfs handler is ever called on a fastrpc file (e.g. by opening and ioctling on /dev/adsprpc-smd). This flag is later used inside of e.g. fastrpc\_internal\_invoke2’s macro invocations of K\_COPY\_FROM\_USER to make decisions about whether the provided pointer is a userland pointer or a kernel-land pointer. However, because the state for making this K\_COPY\_FROM\_USER decision is stored within the broadly accessible fastrpc\_file struct instead of stored per ioctl invocation, this means that 64-bit ioctl invocations of fastrpc\_internal\_invoke2 will use userland provided addresses as kernel pointers if the 32-bit ioctl interface of the same fastrpc\_file was ever previously invoked. This leads directly to attacker-controlled reads of arbitrary kernel addresses.

- [Link](#)

—

” “Mon, 14 Oct 2024

***ABB Cylon Aspect 3.08.00 yumSettings.php Command Injection***

ABB Cylon Aspect version 3.08.00 suffers from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the PROXY HTTP POST parameter called by the yumSettings.php script.

- [Link](#)

—

” “Mon, 14 Oct 2024

***Vivo Fibra Askey RTF8225VW Command Execution***

The Vivo Fibra Askey RTF8225VW modem suffers from an input validation vulnerability that allows for full escalation to a functioning shell once logged in and using the restricted aspsh shell.

- [Link](#)

—

” “Mon, 14 Oct 2024

***WordPress File Manager Advanced Shortcode 2.3.2 Code Injection / Shell Upload***

WordPress File Manager Advanced Shortcode plugin version 2.3.2 suffers from a code injection vulnerability that allows for remote shell upload.

- [Link](#)

—

” “Mon, 14 Oct 2024

***TOTOLINK 9.x Command Injection***

TOTOLINK version 9.x suffers from a remote command injection vulnerability.

- [Link](#)

—

” “Mon, 14 Oct 2024

***MagnusBilling 7.x Command Injection***

MagnusBilling version 7.x suffers from a remote command injection vulnerability.

- [Link](#)

—

” “Mon, 14 Oct 2024

***Bookstore Management System 1.0 SQL Injection***

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

- [Link](#)

—

” “Mon, 14 Oct 2024

***Peel Shopping 2.x Cross Site Scripting / SQL Injection***

Peel Shopping versions 2.x and below 3.1 suffer from cross site scripting and remote SQL injection vulnerabilities. This was already noted discovery in 2012 by Cyber-Crystal but this data provides more details.

- [Link](#)

—

” “Fri, 11 Oct 2024

***ABB Cylon Aspect 3.07.02 user.properties Default Credentials***

ABB Cylon Aspect version 3.07.02 uses a weak set of default administrative credentials that can be guessed in remote password attacks and used to gain full control of the system.

- [Link](#)

—

” “Fri, 11 Oct 2024

***ABB Cylon Aspect 3.08.00 dialupSwitch.php Remote Code Execution***

ABB Cylon Aspect version 3.08.00 suffers from an authenticated OS command injection vulnerability. This can be exploited to inject and execute arbitrary shell commands through the MODEM HTTP POST parameter called by the dialupSwitch.php script.

- [Link](#)

—

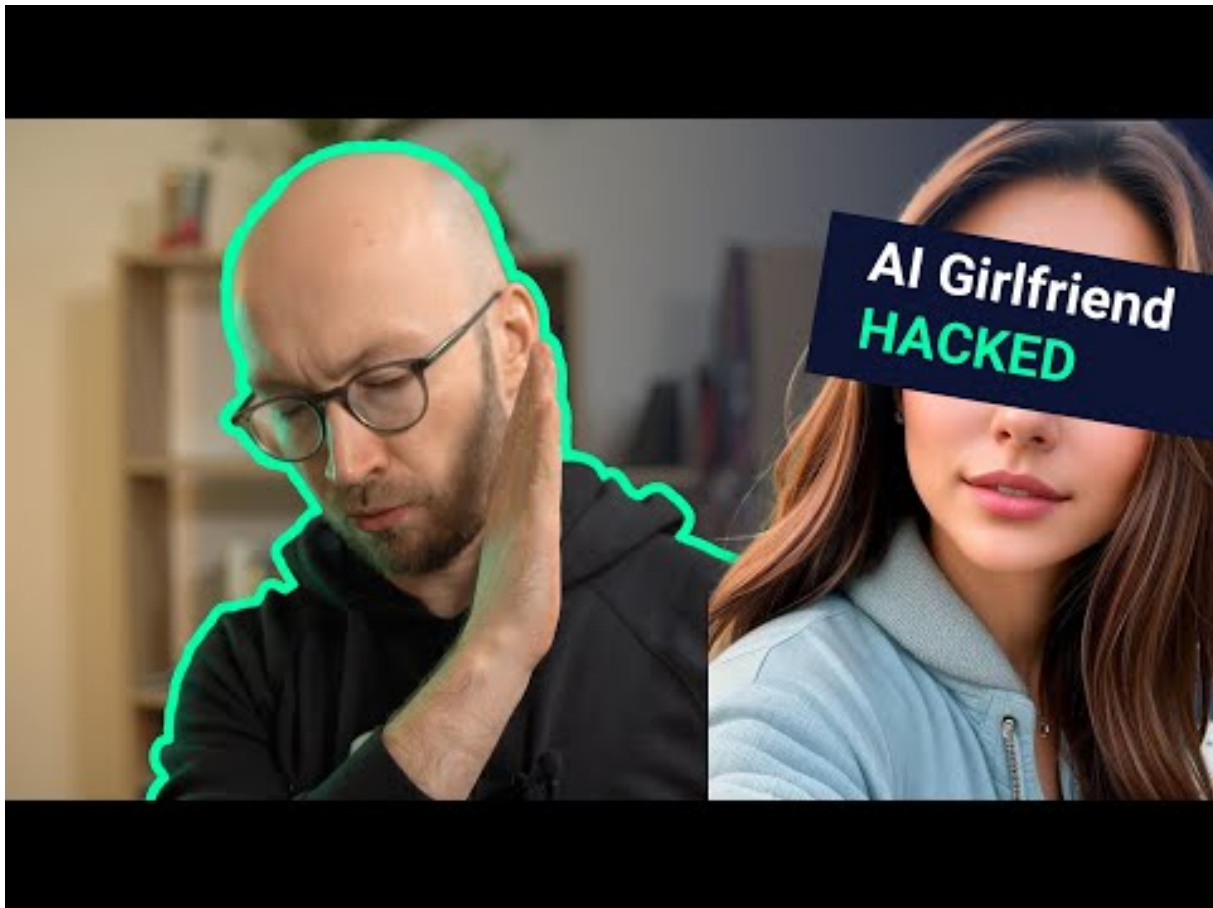
”

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

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor)



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2024-10-22	Sabesp (Companhia de Saneamento Básico do Estado de São Paulo)	[BRA]	<a href="#">Link</a>
2024-10-20	District scolaire public de Winnebago	[USA]	<a href="#">Link</a>
2024-10-19	La Coopérative d'Exploitation et de Répartition Pharmaceutique (CERP) Bretagne-Atlantique	[FRA]	<a href="#">Link</a>
2024-10-18	Grupo Aeroportuario del Centro Norte (OMA)	[MEX]	<a href="#">Link</a>
2024-10-18	Air-e	[COL]	<a href="#">Link</a>
2024-10-17	Formpipe	[DNK]	<a href="#">Link</a>
2024-10-17	Conseil scolaire Viamonde	[CAN]	<a href="#">Link</a>
2024-10-15	aap Implantate AG	[DEU]	<a href="#">Link</a>
2024-10-15	Comune di Aversa	[ITA]	<a href="#">Link</a>
2024-10-14	La mairie de Clairefontaine-en-Yvelines	[FRA]	<a href="#">Link</a>
2024-10-14	Well Chip Group Berhad	[MYS]	<a href="#">Link</a>
2024-10-14	Sorso	[ITA]	<a href="#">Link</a>
2024-10-13	Johannesstift-Diakonie Berlin	[DEU]	<a href="#">Link</a>
2024-10-13	Mutuelle d'Ivry (Mif)	[FRA]	<a href="#">Link</a>
2024-10-11	Calgary Public Library (CPL)	[CAN]	<a href="#">Link</a>
2024-10-11	Polar	[FIN]	<a href="#">Link</a>
2024-10-10	Guajará-Mirim	[BRA]	<a href="#">Link</a>
2024-10-10	Agence pour la Modernisation Administrative (AMA) du Portugal	[PRT]	<a href="#">Link</a>
2024-10-09	Healthcare Services Group (HSG)	[USA]	<a href="#">Link</a>
2024-10-08	Elbe-Heide	[DEU]	<a href="#">Link</a>
2024-10-08	Nevada Joint Union High School District (NJUHSD)	[USA]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-10-08	Les Chambres d'agriculture de Normandie	[FRA]	<a href="#">Link</a>
2024-10-07	Vermilion Parish School System	[USA]	<a href="#">Link</a>
2024-10-07	Axis Health System	[USA]	<a href="#">Link</a>
2024-10-07	Teddy	[ITA]	<a href="#">Link</a>
2024-10-05	Casio Computer Co.	[JPN]	<a href="#">Link</a>
2024-10-04	Groupe Hospi Grand Ouest	[FRA]	<a href="#">Link</a>
2024-10-04	Cabot Financial	[IRL]	<a href="#">Link</a>
2024-10-03	Uttarakhand	[IND]	<a href="#">Link</a>
2024-10-03	American Water Works	[USA]	<a href="#">Link</a>
2024-10-02	Thoraxzentrum Bezirk Unterfranken	[DEU]	<a href="#">Link</a>
2024-10-02	Wayne County	[USA]	<a href="#">Link</a>
2024-10-02	Traffics GmbH	[DEU]	<a href="#">Link</a>
2024-10-02	Berufsschule de Schaffhausen	[CHE]	<a href="#">Link</a>
2024-10-01	Oyonnax	[FRA]	<a href="#">Link</a>
2024-10-01	C.R. Laurence (CRL)	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-23	[shipkar.co.in]	killsec	<a href="#">Link</a>
2024-10-22	[IdeaLab]	hunters	<a href="#">Link</a>
2024-10-22	[Lincoln University (lincolnu.edu)]	fog	<a href="#">Link</a>
2024-10-22	[Clear Connection (clearconnection.com)]	fog	<a href="#">Link</a>
2024-10-22	[Aerotecnic]	blacksuit	<a href="#">Link</a>
2024-10-21	[Precision Steel Services]	spacebears	<a href="#">Link</a>
2024-10-22	[tkg.com]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-22	[lpahorticole.faylbilot.educagri.fr]	ransomhub	<a href="#">Link</a>
2024-10-22	[bwdtechnology.com]	ransomhub	<a href="#">Link</a>
2024-10-16	[davisbrothersinc.com]	ransomhub	<a href="#">Link</a>
2024-10-22	[polypaen.be]	ransomhub	<a href="#">Link</a>
2024-10-22	[dennissupply.com]	ransomhub	<a href="#">Link</a>
2024-10-22	[specpro-inc.com]	ransomhub	<a href="#">Link</a>
2024-10-22	[semna.fr]	ransomhub	<a href="#">Link</a>
2024-10-22	[1doc.sg]	ransomhub	<a href="#">Link</a>
2024-10-22	[Automha]	medusa	<a href="#">Link</a>
2024-10-22	[American Mechanical, inc]	medusa	<a href="#">Link</a>
2024-10-22	[American Medical Billing]	medusa	<a href="#">Link</a>
2024-10-17	[mauguio-carnon.com]	ransomhub	<a href="#">Link</a>
2024-10-09	[donbosco-landser.net]	ransomhub	<a href="#">Link</a>
2024-10-22	[boloforms.com]	killsec	<a href="#">Link</a>
2024-10-22	[onedayevent.com]	killsec	<a href="#">Link</a>
2024-10-22	[autodukan.com]	killsec	<a href="#">Link</a>
2024-10-21	[fordcountrymotors.mx]	lockbit3	<a href="#">Link</a>
2024-10-21	[temple-inc.com]	blackbasta	<a href="#">Link</a>
2024-10-21	[milleredge.com]	blackbasta	<a href="#">Link</a>
2024-10-21	[gkcorp.com]	blackbasta	<a href="#">Link</a>
2024-10-21	[ssbwc.com]	blackbasta	<a href="#">Link</a>
2024-10-21	[lewa.com]	blackbasta	<a href="#">Link</a>
2024-10-04	[City Of Forest Park]	monti	<a href="#">Link</a>
2024-10-21	[Burgess Kilpatrick]	monti	<a href="#">Link</a>
2024-10-21	[Welding and Fabrication (Humble Mfg)]	monti	<a href="#">Link</a>
2024-10-21	[Raeyco Lab Equipment]	monti	<a href="#">Link</a>
2024-10-21	[La Tazza D'oro]	monti	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-21	[Teddy SpA]	blacksuit	<a href="#">Link</a>
2024-10-21	[www.stivo.com]	ransomhub	<a href="#">Link</a>
2024-10-21	[Schweiger Transport (schweiger-gmbh.de)]	fog	<a href="#">Link</a>
2024-10-21	[Philadelphia Macaroni (philamacaroni.com)]	fog	<a href="#">Link</a>
2024-10-21	[yorozu-corp.co.jp]	ransomhub	<a href="#">Link</a>
2024-10-21	[Mercury Theatre]	hunters	<a href="#">Link</a>
2024-10-21	[Trimarc Financial (trimarc.com)]	fog	<a href="#">Link</a>
2024-10-21	[Arango Billboard]	meow	<a href="#">Link</a>
2024-10-21	[Sanglier Limited]	meow	<a href="#">Link</a>
2024-10-20	[qs-group.com]	ransomhub	<a href="#">Link</a>
2024-10-20	[Interbel]	arcusmedia	<a href="#">Link</a>
2024-10-20	[Petropolis Pet Resort]	arcusmedia	<a href="#">Link</a>
2024-10-20	[Superior Quality Insurance Agency]	arcusmedia	<a href="#">Link</a>
2024-10-20	[Vasesa]	arcusmedia	<a href="#">Link</a>
2024-10-20	[Country Club El Bosque]	arcusmedia	<a href="#">Link</a>
2024-10-20	[Atende Software's]	hunters	<a href="#">Link</a>
2024-10-20	[apollohospitals.com]	killsec	<a href="#">Link</a>
2024-10-19	[mh-mech.com]	ransomhub	<a href="#">Link</a>
2024-10-19	[sizeloveconstruction.com]	ransomhub	<a href="#">Link</a>
2024-10-19	[rcschools.net]	blacksuit	<a href="#">Link</a>
2024-10-19	[mopsohio.com]	blacksuit	<a href="#">Link</a>
2024-10-19	[Kansas City Hospice]	blacksuit	<a href="#">Link</a>
2024-10-19	[KMC Controls]	hunters	<a href="#">Link</a>
2024-10-19	[Michael J Gurfinkel]	hunters	<a href="#">Link</a>
2024-10-19	[SPECTRUMCHEMICAL.COM]	clop	<a href="#">Link</a>
2024-10-19	[clinicia.com]	ransomhub	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-19	[paciente.sempremedico.com.br]	ransomhub	<a href="#">Link</a>
2024-10-19	[starhealth.in]	ransomhub	<a href="#">Link</a>
2024-10-19	[T-Space]	cicada3301	<a href="#">Link</a>
2024-10-19	[Pheim Unit Trusts Berhad]	sarcoma	<a href="#">Link</a>
2024-10-19	[Zierick Manufacturing Corporation]	sarcoma	<a href="#">Link</a>
2024-10-19	[Open Range Field Services]	sarcoma	<a href="#">Link</a>
2024-10-19	[ask.vet]	killsec	<a href="#">Link</a>
2024-10-19	[Country Inn & Suites by Radisson]	everest	<a href="#">Link</a>
2024-10-17	[Wilkinson]	play	<a href="#">Link</a>
2024-10-18	[Mid State Electric]	play	<a href="#">Link</a>
2024-10-18	[Absolute Machine Tools]	play	<a href="#">Link</a>
2024-10-18	[McCody]	play	<a href="#">Link</a>
2024-10-18	[The Strainrite Companies]	play	<a href="#">Link</a>
2024-10-05	[INDIBA Group]	cicada3301	<a href="#">Link</a>
2024-10-16	[Astolabs.com]	ransomhub	<a href="#">Link</a>
2024-10-18	[Fromm (FrommBeauty.com)]	fog	<a href="#">Link</a>
2024-10-18	[Ultra Tune (ultratune.com.au)]	fog	<a href="#">Link</a>
2024-10-18	[Alqaryahauction.com]	ransomhub	<a href="#">Link</a>
2024-10-18	[www.qal.com]	ransomhub	<a href="#">Link</a>
2024-10-18	[CreaGen Inc]	everest	<a href="#">Link</a>
2024-10-17	[Dubin Group]	cicada3301	<a href="#">Link</a>
2024-10-17	[RDC Control Ltd]	cicada3301	<a href="#">Link</a>
2024-10-17	[Racing Forensics Inc]	cicada3301	<a href="#">Link</a>
2024-10-17	[Luxwood Software Tools]	cicada3301	<a href="#">Link</a>
2024-10-18	[tripxoxo.com]	killsec	<a href="#">Link</a>
2024-10-17	[www.proflex.ro]	ransomhub	<a href="#">Link</a>
2024-10-17	[www.chiltonisd.org]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-03	[www.kersey.net]	ransomhub	<a href="#">Link</a>
2024-10-02	[www.aristoicclassical.org]	ransomhub	<a href="#">Link</a>
2024-10-03	[www.camelotservices.com]	ransomhub	<a href="#">Link</a>
2024-10-17	[HiCare.net]	ransomhub	<a href="#">Link</a>
2024-10-17	[Bigpharmacy.com.my]	ransomhub	<a href="#">Link</a>
2024-10-17	[Auxit S.r.l.]	sarcoma	<a href="#">Link</a>
2024-10-17	[volohealth.in]	killsec	<a href="#">Link</a>
2024-10-17	[W?!?????n]	play	<a href="#">Link</a>
2024-10-16	[Fractal ID]	stormous	<a href="#">Link</a>
2024-10-02	[Funlab]	lynx	<a href="#">Link</a>
2024-10-09	[Tankstar]	lynx	<a href="#">Link</a>
2024-10-16	[Welker (welker.com)]	fog	<a href="#">Link</a>
2024-10-16	[Cordogan Clark and Associates (cordoganclark.com)]	fog	[Link]((cordoganclark.co
2024-10-15	[powiatjedrzejow.pl]	ransomhub	<a href="#">Link</a>
2024-10-16	[Astolabs.com ASTO LABS]	ransomhub	<a href="#">Link</a>
2024-10-16	[transport-system.com]	ransomhub	<a href="#">Link</a>
2024-10-16	[DoctorsToYou.com]	ransomhub	<a href="#">Link</a>
2024-10-16	[Horsesportireland.ie]	ransomhub	<a href="#">Link</a>
2024-10-16	[Food Sciences Corporation (foodsciences.com)]	fog	<a href="#">Link</a>
2024-10-16	[synertrade.com]	cactus	<a href="#">Link</a>
2024-10-16	[G-plans.com]	ransomhub	<a href="#">Link</a>
2024-10-16	[Fpapak.org]	ransomhub	<a href="#">Link</a>
2024-10-16	[CETRULO]	play	<a href="#">Link</a>
2024-10-16	[Nor-Well]	play	<a href="#">Link</a>
2024-10-16	[Kuhn and Associates]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-16	[moi.gov.ly]	killsec	<a href="#">Link</a>
2024-10-16	[Corporate Job Bank]	bianlian	<a href="#">Link</a>
2024-10-16	[Lein Law Offices]	bianlian	<a href="#">Link</a>
2024-10-15	[Boston Children's Health Physicians]	bianlian	<a href="#">Link</a>
2024-10-15	[Henry County Schools]	rhysida	<a href="#">Link</a>
2024-10-15	[Central Pennsylvania Food Bank]	fog	<a href="#">Link</a>
2024-10-15	[In the depths of software development.]	abyss	<a href="#">Link</a>
2024-10-15	[Promise Technology, Inc.]	abyss	<a href="#">Link</a>
2024-10-15	[basarsoft.com.tr]	ransomhub	<a href="#">Link</a>
2024-10-15	[Ideker]	medusa	<a href="#">Link</a>
2024-10-15	[Ultimate Removal]	medusa	<a href="#">Link</a>
2024-10-15	[Inner City Education Foundation]	medusa	<a href="#">Link</a>
2024-10-15	[SystemPavers]	medusa	<a href="#">Link</a>
2024-10-15	[McMunn & Yates Building Suppliesorp]	sarcoma	<a href="#">Link</a>
2024-10-15	[Microworks]	rhysida	<a href="#">Link</a>
2024-10-15	[Parnell Defense]	hunters	<a href="#">Link</a>
2024-10-15	[Aaren Scientific]	hunters	<a href="#">Link</a>
2024-10-15	[Nora Biscuits]	play	<a href="#">Link</a>
2024-10-15	[Rescar Companies]	play	<a href="#">Link</a>
2024-10-15	[Concord]	play	<a href="#">Link</a>
2024-10-15	[OzarksGo]	play	<a href="#">Link</a>
2024-10-14	[Byerly Aviation]	play	<a href="#">Link</a>
2024-10-14	[Courtney Construction]	play	<a href="#">Link</a>
2024-10-14	[rudrakshahospitals.com]	killsec	<a href="#">Link</a>
2024-10-14	[AOSense]	stormous	<a href="#">Link</a>
2024-10-14	[Henneman Engineering]	play	<a href="#">Link</a>
2024-10-14	[Misionero Vegetables]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-14	[Steel Art Signs]	play	<a href="#">Link</a>
2024-10-14	[Ascires]	stormous	<a href="#">Link</a>
2024-10-14	[Astero]	meow	<a href="#">Link</a>
2024-10-14	[gfm-uk.com]	blackbasta	<a href="#">Link</a>
2024-10-14	[caseparts.com]	blackbasta	<a href="#">Link</a>
2024-10-14	[compra-aruba.com]	ElDorado	<a href="#">Link</a>
2024-10-14	[Durham Region]	dragonforce	<a href="#">Link</a>
2024-10-13	[medicato.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[FUN-LAB]	lynx	<a href="#">Link</a>
2024-10-13	[Cathexis Holdings LP]	interlock	<a href="#">Link</a>
2024-10-11	[Ascires Biomedical Group]	stormous	<a href="#">Link</a>
2024-10-13	[Rocky Mountain Gastroenterology]	meow	<a href="#">Link</a>
2024-10-11	[World Vision Perú]	medusa	<a href="#">Link</a>
2024-10-11	[Construction Systems inc]	medusa	<a href="#">Link</a>
2024-10-13	[Timber]	sarcoma	<a href="#">Link</a>
2024-10-12	[saizeriya.co.jp]	ransomhub	<a href="#">Link</a>
2024-10-12	[Modiin Ezrachi]	meow	<a href="#">Link</a>
2024-10-12	[OSG Tool]	meow	<a href="#">Link</a>
2024-10-11	[NextStage.AI]	ransomhub	<a href="#">Link</a>
2024-10-11	[Volta River Authority]	blacksuit	<a href="#">Link</a>
2024-10-11	[Protective Industrial Products]	hunters	<a href="#">Link</a>
2024-10-11	[Therabel Lucien Pharma SAS]	hunters	<a href="#">Link</a>
2024-10-11	[Rumpke Consolidated Companies]	hunters	<a href="#">Link</a>
2024-10-11	[Østerås Bygg]	medusa	<a href="#">Link</a>
2024-10-11	[Unita Turism]	meow	<a href="#">Link</a>
2024-10-11	[Elmore Goldsmith]	hunters	<a href="#">Link</a>
2024-10-11	[promise.com]	abyss	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-11	[peorialawyers.com]	ransomhub	<a href="#">Link</a>
2024-10-10	[extramarks.com]	killsec	<a href="#">Link</a>
2024-10-10	[Doctors Regional Cancer Center]	incransom	<a href="#">Link</a>
2024-10-10	[oklahomasleepinstitute.co]	threeam	<a href="#">Link</a>
2024-10-10	[Axis Health System]	rhysida	<a href="#">Link</a>
2024-10-10	[The Law Office of Omar O Vargas]	meow	<a href="#">Link</a>
2024-10-10	[Structural and Steel Products]	hunters	<a href="#">Link</a>
2024-10-10	[medexhco.com]	ransomhub	<a href="#">Link</a>
2024-10-10	[La Futura]	meow	<a href="#">Link</a>
2024-10-10	[Barnes Cohen and Sullivan]	meow	<a href="#">Link</a>
2024-10-10	[Atlantic Coast Consulting Inc]	meow	<a href="#">Link</a>
2024-10-10	[Glacier]	hunters	<a href="#">Link</a>
2024-10-09	[Casio Computer Co., Ltd]	underground	<a href="#">Link</a>
2024-10-10	[Doscast]	handala	<a href="#">Link</a>
2024-10-09	[FortyEighty Architecture]	play	<a href="#">Link</a>
2024-10-09	[RobbJack & Crystallume]	play	<a href="#">Link</a>
2024-10-09	[Universal Companies]	play	<a href="#">Link</a>
2024-10-09	[argofinance.org]	killsec	<a href="#">Link</a>
2024-10-09	[transfoodbeverage.com]	killsec	<a href="#">Link</a>
2024-10-09	[InCare Technologies]	sarcoma	<a href="#">Link</a>
2024-10-09	[Antenne Reunion Radio]	sarcoma	<a href="#">Link</a>
2024-10-09	[Smart Media Group Bulgaria]	sarcoma	<a href="#">Link</a>
2024-10-09	[The Roberts Family Law Firm]	sarcoma	<a href="#">Link</a>
2024-10-09	[Gedco]	sarcoma	<a href="#">Link</a>
2024-10-09	[EARTHWORKS Group]	sarcoma	<a href="#">Link</a>
2024-10-09	[Perfection Fresh]	sarcoma	<a href="#">Link</a>
2024-10-09	[Advanced Accounting & Business Advisory]	sarcoma	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-09	[Road Distribution Services]	sarcoma	<a href="#">Link</a>
2024-10-09	[Lácteos Lorán]	sarcoma	<a href="#">Link</a>
2024-10-09	[Curtidos Barbero]	sarcoma	<a href="#">Link</a>
2024-10-09	[EasyPay]	sarcoma	<a href="#">Link</a>
2024-10-09	[Jumbo Electronics Qatar]	sarcoma	<a href="#">Link</a>
2024-10-09	[Navarra & Marzano]	sarcoma	<a href="#">Link</a>
2024-10-09	[Costa Del Sol Hotels]	sarcoma	<a href="#">Link</a>
2024-10-09	[The Plastic Bag]	sarcoma	<a href="#">Link</a>
2024-10-09	[Elevator One]	sarcoma	<a href="#">Link</a>
2024-10-09	[March Elevator]	sarcoma	<a href="#">Link</a>
2024-10-09	[Suntrust Properties]	sarcoma	<a href="#">Link</a>
2024-10-09	[tankstar.com]	lynx	<a href="#">Link</a>
2024-10-09	[victrongroup.com]	abyss	<a href="#">Link</a>
2024-10-09	[FULTON.COM]	clop	<a href="#">Link</a>
2024-10-08	[Orbit Software, Inc.]	dragonforce	<a href="#">Link</a>
2024-10-09	[avans.com]	killsec	<a href="#">Link</a>
2024-10-08	[Eagle Recovery Associates]	play	<a href="#">Link</a>
2024-10-08	[AnVa Industries]	play	<a href="#">Link</a>
2024-10-08	[Smoker's Choice]	play	<a href="#">Link</a>
2024-10-08	[Saratoga Liquor]	play	<a href="#">Link</a>
2024-10-08	[Accounting Resource Group]	play	<a href="#">Link</a>
2024-10-08	[pingan.com]	killsec	<a href="#">Link</a>
2024-10-08	[Ambassador of Israel in Germany Emails]	handala	<a href="#">Link</a>
2024-10-08	[Aaren Scientific]	play	<a href="#">Link</a>
2024-10-04	[blalockcompanies.com]	ransomhub	<a href="#">Link</a>
2024-10-08	[Advantage CDC]	meow	<a href="#">Link</a>
2024-10-08	[Trinity Wholesale Distributors Inc]	meow	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-08	[okcabstract.com]	ransomhub	<a href="#">Link</a>
2024-10-08	[Blain Supply]	lynx	<a href="#">Link</a>
2024-10-07	[Sit & Sleep]	lynx	<a href="#">Link</a>
2024-10-08	[AIUT]	hunters	<a href="#">Link</a>
2024-10-08	[Maxdream]	meow	<a href="#">Link</a>
2024-10-08	[matki.co.uk]	cactus	<a href="#">Link</a>
2024-10-08	[corporatejobbank.com]	cactus	<a href="#">Link</a>
2024-10-08	[Davis Pickren Seydel and Sneed LLP]	meow	<a href="#">Link</a>
2024-10-08	[Accurate Railroad Construction Ltd]	meow	<a href="#">Link</a>
2024-10-08	[Max Shop]	handala	<a href="#">Link</a>
2024-10-07	[autodoc.pro]	ransomhub	<a href="#">Link</a>
2024-10-06	[trulysmall.com]	ransomhub	<a href="#">Link</a>
2024-10-07	[nspproteins.com]	ransomhub	<a href="#">Link</a>
2024-10-08	[The Superior Court of California]	meow	<a href="#">Link</a>
2024-10-08	[healthyuturn.in]	killsec	<a href="#">Link</a>
2024-10-08	[uccretrievals.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[premierpackaging.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[htetech.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[goughconstruction.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[fleetequipment.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[auto-recyclers.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[atd-american.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[allianceind.com]	ElDorado	<a href="#">Link</a>
2024-10-08	[avioesforza.it]	ElDorado	<a href="#">Link</a>
2024-10-08	[tankerska.hr]	ElDorado	<a href="#">Link</a>
2024-10-08	[totalelectronics.com]	ElDorado	<a href="#">Link</a>
2024-10-07	[Istrail]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-07	[Albany College of Pharmacy]	medusa	<a href="#">Link</a>
2024-10-07	[Arelance Group]	medusa	<a href="#">Link</a>
2024-10-08	[Pearl Cohen]	bianlian	<a href="#">Link</a>
2024-10-07	[Broward Realty Corp]	everest	<a href="#">Link</a>
2024-10-07	[yassir.com]	killsec	<a href="#">Link</a>
2024-10-03	[tpgagedcare.com.au]	lockbit3	<a href="#">Link</a>
2024-10-06	[IIB ( Israeli Industrial Batteries ) Leaked]	handala	<a href="#">Link</a>
2024-10-03	[lyra.officegroup]	stormous	<a href="#">Link</a>
2024-10-05	[AOSense/NASA]	stormous	<a href="#">Link</a>
2024-10-05	[NASA/AOSense]	stormous	<a href="#">Link</a>
2024-10-05	[Creative Consumer Concepts]	play	<a href="#">Link</a>
2024-10-05	[Power Torque Services]	play	<a href="#">Link</a>
2024-10-05	[seoulpi.io]	killsec	<a href="#">Link</a>
2024-10-05	[canstarrestorations.com]	ransomhub	<a href="#">Link</a>
2024-10-05	[www.ravencm.com]	ransomhub	<a href="#">Link</a>
2024-10-05	[Ibermutuamur]	hunters	<a href="#">Link</a>
2024-10-05	[betterhalf.ai]	killsec	<a href="#">Link</a>
2024-10-05	[HARTSON-KENNEDY.COM]	clop	<a href="#">Link</a>
2024-10-04	[omniboxx.nl]	ransomhub	<a href="#">Link</a>
2024-10-05	[BNBuilders]	hunters	<a href="#">Link</a>
2024-10-03	[winwinza.com]	ransomhub	<a href="#">Link</a>
2024-10-04	[Storck-Baugesellschaft mbH]	incransom	<a href="#">Link</a>
2024-10-04	[C&L Ward]	play	<a href="#">Link</a>
2024-10-04	[Wilmington Convention Center]	play	<a href="#">Link</a>
2024-10-04	[Guerriere & Halnon]	play	<a href="#">Link</a>
2024-10-04	[Markdom Plastic Products]	play	<a href="#">Link</a>
2024-10-04	[Pete's Road Service]	play	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-03	[release.io]	ransomhub	<a href="#">Link</a>
2024-10-04	[kleberandassociates.com]	ransomhub	<a href="#">Link</a>
2024-10-04	[City Of Forest Park - Full Leak]	monti	<a href="#">Link</a>
2024-10-04	[Riley Gear Corporation]	akira	<a href="#">Link</a>
2024-10-04	[TANYA Creations]	akira	<a href="#">Link</a>
2024-10-04	[mullenwylie.com]	ElDorado	<a href="#">Link</a>
2024-10-04	[GenPro Inc.]	blacksuit	<a href="#">Link</a>
2024-10-04	[CopySmart LLC]	ciphbit	<a href="#">Link</a>
2024-10-04	[North American Breaker]	akira	<a href="#">Link</a>
2024-10-04	[Amplitude Laser]	hunters	<a href="#">Link</a>
2024-10-04	[GW Mechanical]	hunters	<a href="#">Link</a>
2024-10-04	[Dreyfuss + Blackford Architecture]	hunters	<a href="#">Link</a>
2024-10-04	[Transtec SAS]	orca	<a href="#">Link</a>
2024-10-02	[enterpriseoutsourcing.com]	ransomhub	<a href="#">Link</a>
2024-10-04	[DPC DATA]	qilin	<a href="#">Link</a>
2024-10-03	[Lyomark Pharma]	dragonforce	<a href="#">Link</a>
2024-10-03	[Conductive Containers, Inc]	cicada3301	<a href="#">Link</a>
2024-10-04	[bbgc.gov.bd]	killsec	<a href="#">Link</a>
2024-10-03	[CobelPlast]	hunters	<a href="#">Link</a>
2024-10-03	[Shin Bet]	handala	<a href="#">Link</a>
2024-10-03	[Barnes & Cohen]	trinity	<a href="#">Link</a>
2024-10-03	[TRC Worldwide Engineering (Trcww)]	akira	<a href="#">Link</a>
2024-10-03	[Rob Levine & Associates (roblevine.com)]	akira	<a href="#">Link</a>
2024-10-03	[Red Barrels]	nitrogen	<a href="#">Link</a>
2024-10-03	[CaleyWray]	hunters	<a href="#">Link</a>
2024-10-03	[LIFTING.COM]	clop	<a href="#">Link</a>
2024-10-01	[Emerson]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-02	[ETC Companies]	akira	<a href="#">Link</a>
2024-10-02	[Branhaven Chrysler Dodge Jeep Ram]	blacksuit	<a href="#">Link</a>
2024-10-02	[Holmes & Brakel]	akira	<a href="#">Link</a>
2024-10-02	[Forshey Prostok LLP]	qilin	<a href="#">Link</a>
2024-10-02	[Israel Prime Minister Emails]	handala	<a href="#">Link</a>
2024-10-02	[FoccoERP]	trinity	<a href="#">Link</a>
2024-10-01	[Quantum Healthcare]	incransom	<a href="#">Link</a>
2024-10-01	[United Animal Health]	qilin	<a href="#">Link</a>
2024-10-01	[Akromold]	nitrogen	<a href="#">Link</a>
2024-10-01	[Labib Funk Associates]	nitrogen	<a href="#">Link</a>
2024-10-01	[Research Electronics International]	nitrogen	<a href="#">Link</a>
2024-10-01	[Cascade Columbia Distribution]	akira	<a href="#">Link</a>
2024-10-01	[ShoreMaster]	akira	<a href="#">Link</a>
2024-10-01	[marthamedeiros.com.br]	madliberator	<a href="#">Link</a>
2024-10-01	[CSG Consultants]	akira	<a href="#">Link</a>
2024-10-01	[aberdeenwa.gov]	ElDorado	<a href="#">Link</a>
2024-10-01	[Corantioquia]	meow	<a href="#">Link</a>
2024-10-01	[performance-therapies]	qilin	<a href="#">Link</a>
2024-10-01	[www.galab.com]	cactus	<a href="#">Link</a>
2024-10-01	[telehealthcenter.in]	killsec	<a href="#">Link</a>
2024-10-01	[howardcpas.com]	ElDorado	<a href="#">Link</a>
2024-10-01	[bshsoft.com]	ElDorado	<a href="#">Link</a>
2024-10-01	[credihealth.com]	killsec	<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.