

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241016



## 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>21</b>
5.0.1 AI Girlfriends HACKED (Da steht uns noch was bevor) . . . . .	21
<b>6 Cyberangriffe: (Okt)</b>	<b>22</b>
<b>7 Ransomware-Erpressungen: (Okt)</b>	<b>22</b>
<b>8 Quellen</b>	<b>31</b>
8.1 Quellenverzeichnis . . . . .	31
<b>9 Impressum</b>	<b>32</b>

## 1 Editorial

Guten Morgen,

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

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

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

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

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

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

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

#### ***Kritische Sicherheitslücken: Telerik Report Server auf mehreren Wegen angreifbar***

Das Business-Reportingtool Telerik Report Server ist verwundbar. Patches schließen unter anderem eine Schadcode-Lücke.

- [Link](#)

—

#### ***Sicherheitsupdate: Angreifer können Netzwerkanalysetool Wireshark crashen lassen***

Wireshark ist in einer gegen mögliche Angriffe abgesicherten Version erschienen. Darin haben die Entwickler auch mehrere Bugs gefixt.

- [Link](#)

—

#### ***Ransomware: Sophos warnt vor Angriffen auf Veeam-Sicherheitslücke***

Angreifer missbrauchen eine kritische Sicherheitslücke in Veeam, die Codeschmuggel ermöglicht. Davor warnt aktuell Sophos.

- [Link](#)

—

#### ***Sicherheitslücke in Sonicwall SMA1000-Reihe ermöglicht Rechteausweitung***

Sonicwall stopft Sicherheitslücken in SSL-VPN-Appliances der SMA1000-Serie und im Connect-Tunnel-Client. Angreifer können dadurch etwa ihre Rechte ausweiten.

- [Link](#)

—

#### ***CISA warnt vor Sicherheitslücken in 21 IoT-Industrie-Kontrollsystemen***

Die US-IT-Sicherheitsbehörde CISA hat 21 Sicherheitsmeldungen zu industriellen Steuerungssystemen veröffentlicht. IT-Verantwortliche sollten sie prüfen.

- [Link](#)

—

#### ***Anonymisierendes Linux: Tails 6.8.1 kann persistenten Speicher reparieren***

Das zum anonymen Surfen gedachte Tails-Linux schließt in Version 6.8.1 eine Sicherheitslücke. Es verbessert zudem den Umgang mit persistentem Speicher.

- [Link](#)

—

#### ***Juniper: Mehr als 30 Sicherheitslücken gestopft***

Juniper Networks hat mehr als 30 Sicherheitsmitteilungen veröffentlicht. Zugehörige Updates schließen Schwachstellen in Junos OS.

- [Link](#)

---

**Firefox- und Thunderbird-Notfall-Update stopft angegriffenes Sicherheitsleck**

Neue Versionen von Firefox und Thunderbird schließen Sicherheitslücken, die bereits in freier Wildbahn angegriffen werden.

- [Link](#)

---

**Kritische Fortinet-Sicherheitslücke wird angegriffen**

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt, dass eine ältere Lücke in Fortinet-Produkten aktuell angegriffen wird.

- [Link](#)

---

**HP Business-Notebooks: Hotkey-Unterstützung ermöglicht Rechteausweitung**

Hewlett Packard warnt vor einer Schwachstelle im Hotkey-Support von Business-Notebooks. Angreifer können dadurch ihre Rechte ausweiten.

- [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	0.994900000	<a href="#">Link</a>
CVE-2023-6895	0.925010000	0.990710000	<a href="#">Link</a>
CVE-2023-6553	0.948430000	0.993370000	<a href="#">Link</a>
CVE-2023-6019	0.933510000	0.991540000	<a href="#">Link</a>
CVE-2023-52251	0.948240000	0.993360000	<a href="#">Link</a>
CVE-2023-4966	0.970840000	0.998210000	<a href="#">Link</a>
CVE-2023-49103	0.947620000	0.993250000	<a href="#">Link</a>
CVE-2023-48795	0.965360000	0.996530000	<a href="#">Link</a>
CVE-2023-47246	0.960640000	0.995400000	<a href="#">Link</a>
CVE-2023-46805	0.961520000	0.995560000	<a href="#">Link</a>
CVE-2023-46747	0.971910000	0.998570000	<a href="#">Link</a>
CVE-2023-46604	0.971080000	0.998310000	<a href="#">Link</a>
CVE-2023-4542	0.941060000	0.992370000	<a href="#">Link</a>
CVE-2023-43208	0.974200000	0.999510000	<a href="#">Link</a>
CVE-2023-43177	0.954700000	0.994420000	<a href="#">Link</a>
CVE-2023-42793	0.970970000	0.998270000	<a href="#">Link</a>
CVE-2023-41892	0.905460000	0.989170000	<a href="#">Link</a>
CVE-2023-41265	0.920970000	0.990280000	<a href="#">Link</a>
CVE-2023-39143	0.905600000	0.989180000	<a href="#">Link</a>
CVE-2023-38205	0.951890000	0.993940000	<a href="#">Link</a>
CVE-2023-38203	0.964750000	0.996310000	<a href="#">Link</a>
CVE-2023-38146	0.920950000	0.990280000	<a href="#">Link</a>
CVE-2023-38035	0.974600000	0.999680000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967920000	0.997230000	<a href="#">Link</a>
CVE-2023-3519	0.964810000	0.996320000	<a href="#">Link</a>
CVE-2023-35082	0.967900000	0.997230000	<a href="#">Link</a>
CVE-2023-35078	0.969440000	0.997650000	<a href="#">Link</a>
CVE-2023-34993	0.973450000	0.999170000	<a href="#">Link</a>
CVE-2023-34634	0.923140000	0.990500000	<a href="#">Link</a>
CVE-2023-34362	0.970450000	0.998050000	<a href="#">Link</a>
CVE-2023-34105	0.927500000	0.990930000	<a href="#">Link</a>
CVE-2023-34039	0.941110000	0.992390000	<a href="#">Link</a>
CVE-2023-3368	0.934610000	0.991650000	<a href="#">Link</a>
CVE-2023-33246	0.970550000	0.998090000	<a href="#">Link</a>
CVE-2023-32315	0.973230000	0.999090000	<a href="#">Link</a>
CVE-2023-30625	0.953820000	0.994270000	<a href="#">Link</a>
CVE-2023-30013	0.962230000	0.995710000	<a href="#">Link</a>
CVE-2023-29300	0.967820000	0.997190000	<a href="#">Link</a>
CVE-2023-29298	0.969430000	0.997650000	<a href="#">Link</a>
CVE-2023-28432	0.921730000	0.990380000	<a href="#">Link</a>
CVE-2023-28343	0.957650000	0.994910000	<a href="#">Link</a>
CVE-2023-28121	0.922260000	0.990420000	<a href="#">Link</a>
CVE-2023-27524	0.969670000	0.997730000	<a href="#">Link</a>
CVE-2023-27372	0.973980000	0.999420000	<a href="#">Link</a>
CVE-2023-27350	0.968980000	0.997510000	<a href="#">Link</a>
CVE-2023-26469	0.955890000	0.994610000	<a href="#">Link</a>
CVE-2023-26360	0.963280000	0.995940000	<a href="#">Link</a>
CVE-2023-26035	0.967750000	0.997160000	<a href="#">Link</a>
CVE-2023-25717	0.950620000	0.993700000	<a href="#">Link</a>
CVE-2023-25194	0.966130000	0.996710000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.961840000	0.995650000	<a href="#">Link</a>
CVE-2023-24489	0.972860000	0.998940000	<a href="#">Link</a>
CVE-2023-23752	0.949000000	0.993450000	<a href="#">Link</a>
CVE-2023-23333	0.960430000	0.995340000	<a href="#">Link</a>
CVE-2023-22527	0.970410000	0.998030000	<a href="#">Link</a>
CVE-2023-22518	0.962690000	0.995790000	<a href="#">Link</a>
CVE-2023-22515	0.973650000	0.999250000	<a href="#">Link</a>
CVE-2023-21839	0.941470000	0.992420000	<a href="#">Link</a>
CVE-2023-21554	0.952650000	0.994080000	<a href="#">Link</a>
CVE-2023-20887	0.970950000	0.998260000	<a href="#">Link</a>
CVE-2023-1698	0.923310000	0.990540000	<a href="#">Link</a>
CVE-2023-1671	0.962220000	0.995710000	<a href="#">Link</a>
CVE-2023-0669	0.971830000	0.998540000	<a href="#">Link</a>

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

Tue, 15 Oct 2024

#### **[UPDATE] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Tue, 15 Oct 2024

#### **[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—



Tue, 15 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, 15 Oct 2024

**[NEU] [hoch] Apache Camel und mehrere Red Hat Produkte: Mehrere Schwachstellen**

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Apache Camel und in mehreren Red Hat-Produkten ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben und beliebigen Code auszuführen.

- [Link](#)

—

Tue, 15 Oct 2024

**[NEU] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux und Grafana ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Tue, 15 Oct 2024

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

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 15 Oct 2024

**[NEU] [hoch] Kubernetes: Mehrere Schwachstellen ermöglichen Privilegieneskalation**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Kubernetes ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 15 Oct 2024

**[NEU] [hoch] Microsoft GitHub Enterprise: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft GitHub Enterprise ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Tue, 15 Oct 2024

**[NEU] [hoch] Splunk Enterprise: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Splunk Enterprise ausnutzen, um beliebigen Code auszuführen, einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Tue, 15 Oct 2024

**[NEU] [hoch] Nagios Enterprises Nagios XI: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Nagios Enterprises Nagios XI ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Tue, 15 Oct 2024

**[UPDATE] [hoch] Microsoft Azure CLI: Mehrere Schwachstellen ermöglichen Privilegieneskalation und Codeausführung**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure CLI, Microsoft Azure, Microsoft Azure Service Fabric und Microsoft Azure Stack ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- [Link](#)

—

Tue, 15 Oct 2024

**[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Tue, 15 Oct 2024

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

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

- [Link](#)

—

Tue, 15 Oct 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](#)

—

Tue, 15 Oct 2024

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

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

- [Link](#)

—

Tue, 15 Oct 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- [Link](#)

—

Tue, 15 Oct 2024

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

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

- [Link](#)

—

Tue, 15 Oct 2024

**[UPDATE] [hoch] OpenLDAP: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenLDAP ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Tue, 15 Oct 2024

**[UPDATE] [kritisch] Apache Commons: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Tue, 15 Oct 2024

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

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

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/15/2024	[RHEL 8 : firefox (RHSA-2024:8131)]	critical
10/15/2024	[AlmaLinux 8 : thunderbird (ALSA-2024:8024)]	critical
10/15/2024	[AlmaLinux 9 : firefox (ALSA-2024:7958)]	critical
10/15/2024	[AlmaLinux 8 : firefox (ALSA-2024:7977)]	critical
10/15/2024	[AlmaLinux 9 : thunderbird (ALSA-2024:8025)]	critical
10/15/2024	[Google Chrome < 130.0.6723.59 Multiple Vulnerabilities]	critical
10/15/2024	[Google Chrome < 130.0.6723.58 Multiple Vulnerabilities]	critical
10/15/2024	[Google Chrome < 130.0.6723.58 Multiple Vulnerabilities]	critical
10/15/2024	[Ubuntu 14.04 LTS / 16.04 LTS : ImageMagick vulnerabilities (USN-7068-1)]	high
10/15/2024	[RHEL 9 : python3.9 (RHSA-2024:8130)]	high
10/15/2024	[RHEL 9 : skopeo (RHSA-2024:8111)]	high
10/15/2024	[RHEL 9 : containernetworking-plugins (RHSA-2024:8110)]	high
10/15/2024	[AlmaLinux 8 : container-tools:rhel8 (ALSA-2024:8038)]	high
10/15/2024	[RHEL 8 : libuv (RHSA-2024:8132)]	high
10/15/2024	[Security Updates for Azure CLI (October2023)]	high
10/15/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-46804)]	high
10/15/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-46814)]	high

Datum	Schwachstelle	Bewertung
10/15/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-46818)]	high
10/15/2024	[Azul Zulu Java Multiple Vulnerabilities (2024-10-15)]	high
10/15/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7069-1)]	high
10/15/2024	[F5 Networks BIG-IP : Multiple Angular JS vulnerabilities (K000141463)]	high
10/15/2024	[Oracle Linux 9 : skopeo (ELSA-2024-8111)]	high
10/15/2024	[Oracle Linux 9 : containernetworking-plugins (ELSA-2024-8110)]	high
10/15/2024	[Festo (CVE-2020-12069)]	high
10/15/2024	[Wago (CVE-2020-12069)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“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 Injectin / 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](#)

—

” “Fri, 11 Oct 2024

***ABB Cylon Aspect 3.07.02 sshUpdate.php Unauthenticated Remote SSH Service Control***

ABB Cylon Aspect version 3.07.02 suffers from a vulnerability that allows an unauthenticated attacker to enable or disable the SSH daemon by sending a POST request to sshUpdate.php with a simple JSON payload. This can be exploited to start the SSH service on the remote host without proper authentication, potentially enabling unauthorized access or stop and deny service access.

- [Link](#)

—

” “Fri, 11 Oct 2024

***TerraMaster TOS 4.2.29 Code Injection / Local File Inclusion***

TerraMaster TOS version 4.2.29 suffers from a remote code injection vulnerability leveraging a local file inclusion vulnerability.

- [Link](#)

—

” “Fri, 11 Oct 2024

***SolarView Compact 6.00 Code Injection***

SolarView Compact version 6.00 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Fri, 11 Oct 2024

***Openfire 4.8.0 Code Injection***

Openfire version 4.8.0 suffers from authentication bypass and code injection vulnerabilities.

- [Link](#)

—

” “Fri, 11 Oct 2024

***MagnusBilling 6.x Code Injection***

MagnusBilling version 6.x suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Fri, 11 Oct 2024

***Kafka UI 0.7.1 Code Injection***

Kafka UI version 0.7.1 suffers from a remote code injection vulnerability.

- [Link](#)

—

” “Fri, 11 Oct 2024

***GL.iNet 4.4.3 Code Injection***

GL.iNet version 4.4.3 suffers from authentication bypass and code injection vulnerabilities.

- [Link](#)

—

” “Fri, 11 Oct 2024

***Gibbon School Platform 26.0.00 Code Injection***

Gibbon School Platform version 26.0.00 suffers from a PHP code injection vulnerability.

- [Link](#)

—



” “Fri, 11 Oct 2024

**Craft CMS 4.4.14 Code Injection**

Craft CMS version 4.4.14 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Fri, 11 Oct 2024

**Chamilo 1.11.18 Code Injection**

Chamilo version 1.11.18 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Fri, 11 Oct 2024

**Artica Proxy 4.40 Code Injection**

Artica Proxy version 4.40 suffers from a code injection vulnerability that provides a reverse shell.

- [Link](#)

—

” “Thu, 10 Oct 2024

**ABB Cylon Aspect 3.08.01 persistenceManagerAjax.php Directory Traversal**

ABB Cylon Aspect version 3.08.01 has a directory traversal vulnerability that can be exploited by an unauthenticated attacker to list the contents of arbitrary directories without reading file contents, leading to information disclosure of directory structures and filenames. This may expose sensitive system details, aiding in further attacks. The issue lies in the listFiles() function of the persistenceManagerAjax.php script, which calls PHP’s readdir() function without proper input validation of the directory POST parameter.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Tue, 15 Oct 2024

**ZDI-24-1411: Delta Electronics CNCSoft-G2 DPAX File Parsing Uninitialized Variable Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1410: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1409: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1408: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1407: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1406: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1405: Delta Electronics CNCSoft-G2 ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1404: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1403: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1402: Delta Electronics CNCSoft-G2 DOPSoft DPAX File Parsing Stack-based Buffer Overflow***

**Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1401: Delta Electronics CNCSoft-G2 DOPSoft DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1400: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1399: Delta Electronics CNCSoft-G2 DPAX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1398: Delta Electronics CNCSoft-G2 DOPSoft ALM File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1397: Delta Electronics CNCSoft-G2 DOPSoft CMT File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1396: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

**ZDI-24-1395: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1394: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1393: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1392: Delta Electronics CNCSoft-G2 DPAX File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1391: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1390: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1389: Delta Electronics CNCSoft-G2 DPAX File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1388: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1387: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1386: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1385: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1384: Delta Electronics CNCSoft-G2 DPAX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1383: PostHog database\_schema Server-Side Request Forgery Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 15 Oct 2024

***ZDI-24-1382: QEMU SCSI Use-After-Free Local Privilege Escalation Vulnerability***

- [Link](#)

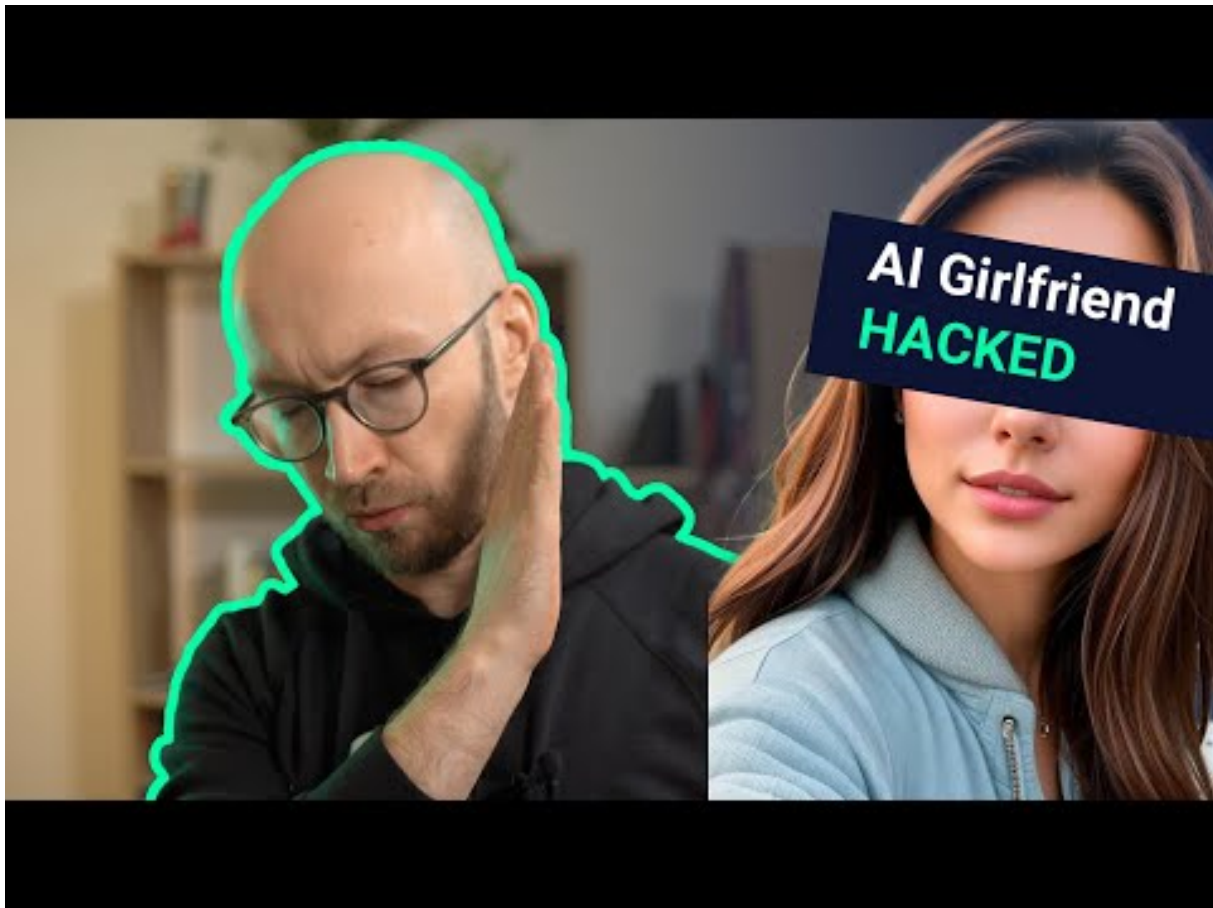
—

”

## 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
2024-10-13	Johannesstift-Diakonie Berlin	[DEU]	<a href="#">Link</a>
2024-10-11	Calgary Public Library (CPL)	[CAN]	<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>
2024-10-08	Elbe-Heide	[DEU]	<a href="#">Link</a>
2024-10-08	Nevada Joint Union High School District (NJUHSD)	[USA]	<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>
2024-10-05	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>
2024-10-01	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
2024-10-16	[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>
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	[In the depths of software development. Unlocking the secrets of 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>



Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>
2024-10-14	[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	[confidencegroup.com.bd]	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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-11	[practicesuite.us]	ransomhub	<a href="#">Link</a>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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]	clon	<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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>
2024-10-07	[trulysmall.com]	ransomhub	<a href="#">Link</a>
2024-10-07	[nspproteins.com]	ransomhub	<a href="#">Link</a>
2024-10-07	[Richmond Auto Mall - Full Leak]	monti	<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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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.it]	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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-04	[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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-02	[domainindustries.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[ironmetals.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[rollxvans.com]	ransomhub	<a href="#">Link</a>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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.