

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241020



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	11
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>13</b>
4.1 Exploits der letzten 5 Tage . . . . .	13
4.2 0-Days der letzten 5 Tage . . . . .	17
<b>5 Die Hacks der Woche</b>	<b>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>32</b>
8.1 Quellenverzeichnis . . . . .	32
<b>9 Impressum</b>	<b>33</b>

## 1 Editorial

Guten Morgen,

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

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

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

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

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

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

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

#### ***Kritische Sicherheitslücke: 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](#)

---

#### ***Sicherheitsupdates: Root-Attacken auf VoIP-Adapter von Cisco möglich***

Angreifer können mehrere Produkte von Cisco attackieren und im schlimmsten Fall Systeme kompromittieren.

- [Link](#)

---

#### ***F5 BIG-IP: Zugriffsbeschränkungen umgehbar***

F5 hat eine Sicherheitslücke in der Monitor-Funktion von BIG-IP gemeldet. Angreifer können betroffene Systeme kompromittieren.

- [Link](#)

---

#### ***Solarwinds: Lücken in Plattform und Serv-U ermöglichen Schadcode-Schmuggel***

Solarwinds warnt vor Sicherheitslücken in der Plattform und in Serv-U. Angreifer können etwa Code einschleusen oder ihre Rechte ausweiten.

- [Link](#)

---

#### ***VMware HCX: Codeschmuggel durch SQL-Injection-Lücke möglich***

Broadcom hat mit einem Update eine Sicherheitslücke in VMware HCX geschlossen. Angreifer können durch sie Code einschleusen und ausführen.

- [Link](#)

---

#### ***Sicherheitsupdate: Zwei Drucker-Modelle aus HPs DesignJet-Serie attackierbar***

Setzen Angreifer erfolgreich an einer Sicherheitslücke in bestimmten HP-Druckern an, können sie eigentlich abgeschottete Informationen einsehen.

- [Link](#)

---

---

**Jetzt patchen! Angreifer attackieren Solarwinds Web Help Desk**

Derzeit laufen Attacken auf die Kundensupport-Software Web Help Desk von Solarwinds. Sicherheitsupdates stehen zum Download.

- [Link](#)

---

**Github Enterprise Server: Angreifer können Authentifizierung umgehen**

Unter bestimmten Voraussetzungen sind unbefugte Zugriffe auf Github Enterprise Server möglich. Sicherheitsupdates sind verfügbar.

- [Link](#)

---

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

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

- [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	0.994910000	<a href="#">Link</a>
CVE-2023-6895	0.925010000	0.990730000	<a href="#">Link</a>
CVE-2023-6553	0.948430000	0.993390000	<a href="#">Link</a>
CVE-2023-6019	0.933700000	0.991590000	<a href="#">Link</a>
CVE-2023-6018	0.911590000	0.989650000	<a href="#">Link</a>
CVE-2023-52251	0.948240000	0.993380000	<a href="#">Link</a>
CVE-2023-4966	0.971220000	0.998380000	<a href="#">Link</a>
CVE-2023-49103	0.947620000	0.993270000	<a href="#">Link</a>
CVE-2023-48795	0.965360000	0.996540000	<a href="#">Link</a>
CVE-2023-47246	0.960640000	0.995410000	<a href="#">Link</a>
CVE-2023-46805	0.961520000	0.995580000	<a href="#">Link</a>
CVE-2023-46747	0.971910000	0.998570000	<a href="#">Link</a>
CVE-2023-46604	0.971080000	0.998320000	<a href="#">Link</a>
CVE-2023-4542	0.941060000	0.992420000	<a href="#">Link</a>
CVE-2023-43208	0.974200000	0.999510000	<a href="#">Link</a>
CVE-2023-43177	0.954040000	0.994310000	<a href="#">Link</a>
CVE-2023-42793	0.970970000	0.998270000	<a href="#">Link</a>
CVE-2023-41892	0.905460000	0.989200000	<a href="#">Link</a>
CVE-2023-41265	0.920970000	0.990310000	<a href="#">Link</a>
CVE-2023-39143	0.905600000	0.989210000	<a href="#">Link</a>
CVE-2023-38205	0.954790000	0.994420000	<a href="#">Link</a>
CVE-2023-38203	0.964750000	0.996310000	<a href="#">Link</a>
CVE-2023-38146	0.920950000	0.990300000	<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	0.996330000	<a href="#">Link</a>
CVE-2023-35082	0.967900000	0.997240000	<a href="#">Link</a>
CVE-2023-35078	0.967840000	0.997210000	<a href="#">Link</a>
CVE-2023-34993	0.973050000	0.999000000	<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	0.990950000	<a href="#">Link</a>
CVE-2023-34039	0.941110000	0.992430000	<a href="#">Link</a>
CVE-2023-3368	0.937940000	0.992060000	<a href="#">Link</a>
CVE-2023-33246	0.970550000	0.998120000	<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	0.995720000	<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	0.990390000	<a href="#">Link</a>
CVE-2023-28343	0.957970000	0.994960000	<a href="#">Link</a>
CVE-2023-28121	0.922260000	0.990420000	<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	0.997530000	<a href="#">Link</a>
CVE-2023-26469	0.955890000	0.994620000	<a href="#">Link</a>
CVE-2023-26360	0.963280000	0.995940000	<a href="#">Link</a>
CVE-2023-26035	0.967750000	0.997170000	<a href="#">Link</a>
CVE-2023-25717	0.950620000	0.993710000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.966130000	0.996710000	<a href="#">Link</a>
CVE-2023-2479	0.961840000	0.995660000	<a href="#">Link</a>
CVE-2023-24489	0.972860000	0.998930000	<a href="#">Link</a>
CVE-2023-23752	0.949000000	0.993480000	<a href="#">Link</a>
CVE-2023-23333	0.960430000	0.995340000	<a href="#">Link</a>
CVE-2023-22527	0.970410000	0.998050000	<a href="#">Link</a>
CVE-2023-22518	0.962690000	0.995810000	<a href="#">Link</a>
CVE-2023-22515	0.973650000	0.999250000	<a href="#">Link</a>
CVE-2023-21839	0.941470000	0.992470000	<a href="#">Link</a>
CVE-2023-21554	0.952650000	0.994080000	<a href="#">Link</a>
CVE-2023-20887	0.970950000	0.998270000	<a href="#">Link</a>
CVE-2023-1698	0.923310000	0.990550000	<a href="#">Link</a>
CVE-2023-1671	0.962220000	0.995720000	<a href="#">Link</a>
CVE-2023-0669	0.971830000	0.998540000	<a href="#">Link</a>

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

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](#)

—

Fri, 18 Oct 2024

#### **[UPDATE] [hoch] Cisco Analog Telephone Adaptor (ATA): Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen im Cisco Analog Telephone Adaptor ATA 191 und ATA 192 ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen oder einen Denial-of-



Service-Zustand zu erzeugen.

- [Link](#)

—

Fri, 18 Oct 2024

**[NEU] [UNGEPATCHT] [hoch] D-LINK Router: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstelle in D-LINK Router ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 18 Oct 2024

**[NEU] [hoch] Grafana: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Fri, 18 Oct 2024

**[UPDATE] [hoch] International Components for Unicode (ICU): Schwachstelle ermöglichen Ausführen von beliebigem Programmcode mit Benutzerrechten**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in der Bibliothek ICU ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.

- [Link](#)

—

Fri, 18 Oct 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Fri, 18 Oct 2024

**[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 18 Oct 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um

vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Fri, 18 Oct 2024

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

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

- [Link](#)

—

Fri, 18 Oct 2024

**[UPDATE] [hoch] Oracle Construction and Engineering: Mehrere Schwachstellen**

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle Construction and Engineering ausnutzen, um die Vertraulichkeit und Integrität zu gefährden.

- [Link](#)

—

Fri, 18 Oct 2024

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

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

- [Link](#)

—

Fri, 18 Oct 2024

**[UPDATE] [kritisch] Veeam Backup & Replication: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Veeam Backup & Replication ausnutzen, um Dateien zu manipulieren, erweiterte Rechte zu erlangen, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen preiszugeben.

- [Link](#)

—

Fri, 18 Oct 2024

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

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

- [Link](#)

—

Fri, 18 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](#)

—

Fri, 18 Oct 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS cups-browsed ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 18 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](#)

—

Fri, 18 Oct 2024

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

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

- [Link](#)

—

Thu, 17 Oct 2024

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

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

- [Link](#)

—

Thu, 17 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](#)

—  
Thu, 17 Oct 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen ermöglichen Manipulation von Dateien**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
10/19/2024	[Fedora 39 : thunderbird (2024-18ac02a385)]	critical
10/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:3731-1)]	critical
10/18/2024	[Oracle Database Server (October 2024 CPU)]	critical
10/18/2024	[Docker for Windows < 4.34.3 RCE]	critical
10/18/2024	[Docker Desktop < 4.34.3 RCE (macOS)]	critical
10/18/2024	[Docker Desktop < 4.34.3 RCE]	critical
10/19/2024	[SUSE SLES15 / openSUSE 15 Security Update : php7 (SUSE-SU-2024:3733-1)]	high
10/19/2024	[Fedora 39 : rust-hyper-rustls / rust-reqwest / rust-rustls-native-certs / etc (2024-ff98facbc6)]	high
10/19/2024	[Fedora 40 : libdigidocpp (2024-f7a5b49a73)]	high
10/19/2024	[Fedora 40 : oath-toolkit (2024-cb2e1f0168)]	high
10/19/2024	[Fedora 40 : chromium (2024-4d80983af6)]	high
10/19/2024	[Fedora 40 : libarchive (2024-80e4603b92)]	high
10/19/2024	[Fedora 40 : rust-hyper-rustls / rust-reqwest / rust-rustls-native-certs / etc (2024-bf524bf5c0)]	high

Datum	Schwachstelle	Bewertung
10/19/2024	[Fedora 39 : oath-toolkit (2024-dad1d2b46a)]	high
10/19/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0337-1)]	high
10/19/2024	[SUSE SLES12 Security Update : php74 (SUSE-SU-2024:3732-1)]	high
10/19/2024	[SUSE SLES15 / openSUSE 15 Security Update : php8 (SUSE-SU-2024:3729-1)]	high
10/19/2024	[openSUSE 15 Security Update : python-starlette (SUSE-SU-2024:3719-1)]	high
10/19/2024	[Photon OS 5.0: Wireshark PHSA-2024-5.0-0385]	high
10/19/2024	[Debian dla-3923 : php-horde-turba - security update]	high
10/19/2024	[Fedora 39 : chromium (2024-c0b1d26de3)]	high
10/18/2024	[Autodesk Revit 2024.x < 2024.2.2 / 2025.x < 2025.3 PDF File Parsing Out-of-Bounds Write (ADSK-SA-2024-0018)]	high
10/18/2024	[Autodesk Revit 2024.x < 2024.3 / 2025.x < 2025.3 RFA File Parsing Buffer Overflow (ADSK-SA-2024-0017)]	high
10/18/2024	[FreeBSD : electron{31,32} – multiple vulnerabilities (815bf172-ab9e-4c4b-9662-d18b0054330d)]	high
10/18/2024	[Mattermost Server 9.5.x < 9.5.8 / 9.8.x < 9.8.3 / 9.9.x < 9.9.2 / 9.10.x < 9.10.1 (MMSA-2024-00368)]	high
10/18/2024	[Mattermost Server 9.5.x < 9.5.8 / 9.8.x < 9.8.3 / 9.9.x < 9.9.2 / 9.10.x < 9.10.1 (MMSA-2024-00374)]	high
10/18/2024	[Oracle Linux 8 / 9 : java-17-openjdk (ELSA-2024-8124)]	high
10/18/2024	[Oracle Linux 8 / 9 : java-1.8.0-openjdk (ELSA-2024-8117)]	high
10/18/2024	[actionmailer Ruby Library 3.x < 6.1.7.9 / 7.0.x < 7.0.8.5 / 7.1.x < 7.1.4.1 / 7.2.x < 7.2.1.1 DoS (CVE-2024-47889)]	high
10/18/2024	[CBL Mariner 2.0 Security Update: libarchive (CVE-2024-48958)]	high
10/18/2024	[CBL Mariner 2.0 Security Update: libarchive (CVE-2024-48957)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“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 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](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Fri, 18 Oct 2024

**ZDI-24-1420: Schneider Electric EcoStruxure Data Center Expert XML External Entity Processing Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 17 Oct 2024

**ZDI-24-1419: Trend Micro Deep Security Improper Access Control Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Thu, 17 Oct 2024

**ZDI-24-1418: Trend Micro Cloud Edge REST API Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 17 Oct 2024

**ZDI-24-1417: Schneider Electric EcoStruxure Data Center Expert Improper Verification of Crypto-**

***graphic Signature Remote Code Execution Vulnerability***

- [Link](#)

—

” “Thu, 17 Oct 2024

***ZDI-24-1416: Schneider Electric EcoStruxure Data Center Expert Missing Authentication Information Disclosure Vulnerability***

- [Link](#)

—

” “Thu, 17 Oct 2024

***ZDI-24-1415: Schneider Electric Zelio Soft 2 ZM2 File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

—

” “Thu, 17 Oct 2024

***ZDI-24-1414: Oracle VirtualBox BusLogic Uninitialized Memory Information Disclosure Vulnerability***

- [Link](#)

—

” “Thu, 17 Oct 2024

***ZDI-24-1413: Oracle VirtualBox TPM Heap-based Buffer Overflow Local Privilege Escalation Vulnerability***

- [Link](#)

—

” “Thu, 17 Oct 2024

***ZDI-24-1412: Oracle VirtualBox Shared Folders Incorrect Authorization Local Privilege Escalation Vulnerability***

- [Link](#)

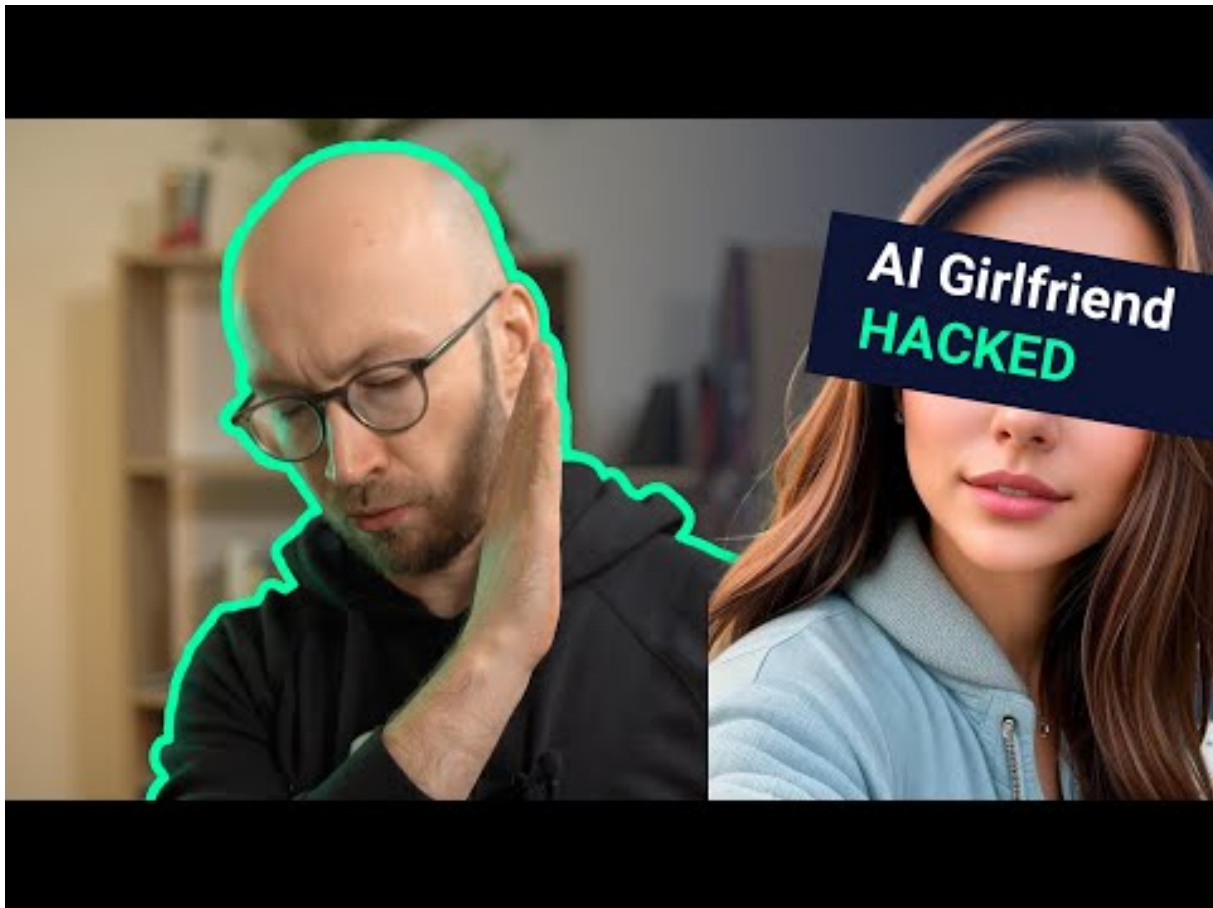
—

”

## 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
2024-10-18	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>
2024-10-11	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>
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>

Datum	Opfer	Land	Information
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
2024-10-20	[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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-18	[INDIBA Group]	cicada3301	<a href="#">Link</a>
2024-10-16	[Astolabs.com]	ransomhub	<a href="#">Link</a>
2024-10-18	[Neighbors Credit Union]	blacksuit	<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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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?l????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	<a href="#">[Link]((cordoganclark.co</a>
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>
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>



Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[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>
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	[peorialawyers.com]	ransomhub	<a href="#">Link</a>
2024-10-10	[extramarks.com]	killsec	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-09	[Road Distribution Services]	sarcoma	<a href="#">Link</a>
2024-10-09	[Lácteos Lorán]	sarcoma	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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]	cllop	<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>
2024-10-08	[okcabstract.com]	ransomhub	<a href="#">Link</a>
2024-10-08	[Blain Supply]	lynx	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-04	[release.io]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-10-02	[rollxvans.com]	ransomhub	<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.