


---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250511



## 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) . . . . .	9
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	12
<b>4 Die Hacks der Woche</b>	<b>14</b>
4.0.1 Information Stealer. Wie funktionieren sie? . . . . .	15
<b>5 Cyberangriffe: (Mai)</b>	<b>16</b>
<b>6 Ransomware-Erpressungen: (Mai)</b>	<b>16</b>
<b>7 Quellen</b>	<b>21</b>
7.1 Quellenverzeichnis . . . . .	21
<b>8 Impressum</b>	<b>22</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

#### ***Apple AirPlay: Sicherheitsforscher warnen vor gravierenden Lücken***

Schwachstellen erlauben die Übernahme von AirPlay-Geräten, warnen Sicherheitsforscher. Für iPhones & Co gibt es Patches, bei anderer Hardware wird es knifflig.

- [Link](#)

—

#### ***Docker: Rechteausweitungslücke in Desktop für Windows***

Angreifer können ihre Rechte durch ein Sicherheitsleck in Docker Desktop für Windows ausweiten. Ein Update korrigiert das.

- [Link](#)

—

#### ***Seiko-Epson-Druckertreiber ermöglicht Rechteausweitung auf System***

Die Windows-Druckertreiber für Seiko-Epson-Drucker enthalten eine hochriskante Lücke, die Angreifern die Ausweitung ihrer Rechte ermöglicht.

- [Link](#)

—

#### ***Attackierte SAP-Lücke: Hunderte verwundbare Server im Netz***

Am Freitag hat SAP eine bereits angegriffene Sicherheitslücke in SAP Netweaver gepatcht. Noch immer sind hunderte Server verwundbar.

- [Link](#)

—

#### ***Angriffe auf Sicherheitslücken in Commvault, Brocade Fabric OS und Active! Mail***

Angreifer nehmen junge Schwachstellen in Commvault, Brocade Fabric OS und Active! Mail ins Visier und kompromittieren Systeme.

- [Link](#)

—

#### ***Sicherheitslücken: Attacken auf Lernplattform Moodle können bevorstehen***

Mehrere Softwareschwachstellen gefährden Moodle-Instanzen. Sicherheitsupdates stehen zum Download bereit.

- [Link](#)

—

#### ***Sicherheitsupdate: Unbefugte Zugriffe auf Spring Boot möglich***

Admins sollten Softwareentwicklungsumgebungen mit Spring Boot aus Sicherheitsgründen auf den aktuellen Stand bringen.

- [Link](#)

---

**Connectwise Screenconnect: Hochriskante Codeschmuggel-Lücke**

In Connectwise Screenconnect schließt der Hersteller mit einem Update eine als hohes Risiko eingestufte Schadcode-Lücke.

- [Link](#)

---

**Sicherheitsupdate: Nvidia-Grafikkartentreiber unter Linux angreifbar**

Drei Sicherheitslücken gefährden PCs mit einer Grafikkarte von Nvidia. Im schlimmsten Fall kann Schadcode auf Linux-Systeme gelangen.

- [Link](#)

---

**SAP patcht attackierte, kritische Schwachstelle außer der Reihe**

Eine kritische Sicherheitslücke nötigt SAP zum Update außer der Reihe. Sie wird bereits in freier Wildbahn angegriffen.

- [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-2025-3248	0.911750000	0.996130000	<a href="#">Link</a>
CVE-2025-29927	0.924340000	0.997120000	<a href="#">Link</a>
CVE-2025-24893	0.924030000	0.997090000	<a href="#">Link</a>
CVE-2025-24813	0.937100000	0.998360000	<a href="#">Link</a>
CVE-2025-0282	0.928560000	0.997490000	<a href="#">Link</a>
CVE-2025-0108	0.936630000	0.998310000	<a href="#">Link</a>
CVE-2024-9989	0.911880000	0.996140000	<a href="#">Link</a>
CVE-2024-9935	0.928150000	0.997430000	<a href="#">Link</a>
CVE-2024-9474	0.942830000	0.999250000	<a href="#">Link</a>
CVE-2024-9465	0.942440000	0.999150000	<a href="#">Link</a>
CVE-2024-9463	0.942640000	0.999220000	<a href="#">Link</a>
CVE-2024-9264	0.920720000	0.996800000	<a href="#">Link</a>
CVE-2024-9234	0.925020000	0.997170000	<a href="#">Link</a>
CVE-2024-9047	0.914320000	0.996300000	<a href="#">Link</a>
CVE-2024-9014	0.923220000	0.997010000	<a href="#">Link</a>
CVE-2024-8963	0.943720000	0.999540000	<a href="#">Link</a>
CVE-2024-8856	0.917780000	0.996550000	<a href="#">Link</a>
CVE-2024-8504	0.923140000	0.996990000	<a href="#">Link</a>
CVE-2024-8503	0.930440000	0.997680000	<a href="#">Link</a>
CVE-2024-8190	0.930530000	0.997690000	<a href="#">Link</a>
CVE-2024-7954	0.939410000	0.998660000	<a href="#">Link</a>
CVE-2024-7928	0.914030000	0.996280000	<a href="#">Link</a>
CVE-2024-7593	0.943990000	0.999690000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7120	0.912160000	0.996150000	<a href="#">Link</a>
CVE-2024-6911	0.927560000	0.997380000	<a href="#">Link</a>
CVE-2024-6782	0.937140000	0.998370000	<a href="#">Link</a>
CVE-2024-6781	0.933010000	0.997960000	<a href="#">Link</a>
CVE-2024-6670	0.944670000	0.999930000	<a href="#">Link</a>
CVE-2024-6646	0.921240000	0.996860000	<a href="#">Link</a>
CVE-2024-5932	0.941040000	0.998910000	<a href="#">Link</a>
CVE-2024-5910	0.908210000	0.995890000	<a href="#">Link</a>
CVE-2024-5806	0.907610000	0.995850000	<a href="#">Link</a>
CVE-2024-57727	0.934600000	0.998090000	<a href="#">Link</a>
CVE-2024-56145	0.915340000	0.996360000	<a href="#">Link</a>
CVE-2024-55956	0.932330000	0.997890000	<a href="#">Link</a>
CVE-2024-55591	0.930070000	0.997640000	<a href="#">Link</a>
CVE-2024-53704	0.936990000	0.998350000	<a href="#">Link</a>
CVE-2024-53677	0.918940000	0.996660000	<a href="#">Link</a>
CVE-2024-5217	0.941960000	0.999080000	<a href="#">Link</a>
CVE-2024-51567	0.942610000	0.999200000	<a href="#">Link</a>
CVE-2024-51378	0.939560000	0.998690000	<a href="#">Link</a>
CVE-2024-5084	0.907680000	0.995850000	<a href="#">Link</a>
CVE-2024-50623	0.939920000	0.998740000	<a href="#">Link</a>
CVE-2024-50603	0.942990000	0.999290000	<a href="#">Link</a>
CVE-2024-50498	0.924360000	0.997120000	<a href="#">Link</a>
CVE-2024-50379	0.919360000	0.996700000	<a href="#">Link</a>
CVE-2024-4956	0.939760000	0.998720000	<a href="#">Link</a>
CVE-2024-48914	0.909810000	0.996000000	<a href="#">Link</a>
CVE-2024-4885	0.942780000	0.999240000	<a href="#">Link</a>
CVE-2024-4879	0.943360000	0.999400000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-48307	0.909650000	0.995980000	<a href="#">Link</a>
CVE-2024-48248	0.934500000	0.998070000	<a href="#">Link</a>
CVE-2024-47575	0.909990000	0.996000000	<a href="#">Link</a>
CVE-2024-47176	0.916890000	0.996480000	<a href="#">Link</a>
CVE-2024-46938	0.919470000	0.996710000	<a href="#">Link</a>
CVE-2024-4577	0.943760000	0.999550000	<a href="#">Link</a>
CVE-2024-45519	0.941500000	0.998980000	<a href="#">Link</a>
CVE-2024-45388	0.915030000	0.996340000	<a href="#">Link</a>
CVE-2024-45216	0.939010000	0.998610000	<a href="#">Link</a>
CVE-2024-45195	0.940810000	0.998880000	<a href="#">Link</a>
CVE-2024-4443	0.933810000	0.998020000	<a href="#">Link</a>
CVE-2024-4439	0.912420000	0.996170000	<a href="#">Link</a>
CVE-2024-44000	0.920120000	0.996770000	<a href="#">Link</a>
CVE-2024-4358	0.942540000	0.999180000	<a href="#">Link</a>
CVE-2024-43451	0.910720000	0.996060000	<a href="#">Link</a>
CVE-2024-42640	0.904770000	0.995670000	<a href="#">Link</a>
CVE-2024-4257	0.922930000	0.996980000	<a href="#">Link</a>
CVE-2024-41713	0.939620000	0.998700000	<a href="#">Link</a>
CVE-2024-41107	0.929020000	0.997530000	<a href="#">Link</a>
CVE-2024-4040	0.944120000	0.999720000	<a href="#">Link</a>
CVE-2024-40348	0.916690000	0.996460000	<a href="#">Link</a>
CVE-2024-39914	0.926650000	0.997300000	<a href="#">Link</a>
CVE-2024-38856	0.943660000	0.999510000	<a href="#">Link</a>
CVE-2024-38816	0.927560000	0.997380000	<a href="#">Link</a>
CVE-2024-38475	0.929350000	0.997560000	<a href="#">Link</a>
CVE-2024-38112	0.917790000	0.996550000	<a href="#">Link</a>
CVE-2024-37032	0.919920000	0.996750000	<a href="#">Link</a>



CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-36412	0.934710000	0.998100000	<a href="#">Link</a>
CVE-2024-36401	0.944180000	0.999750000	<a href="#">Link</a>
CVE-2024-36104	0.938050000	0.998490000	<a href="#">Link</a>
CVE-2024-3552	0.932020000	0.997850000	<a href="#">Link</a>
CVE-2024-3495	0.932990000	0.997950000	<a href="#">Link</a>
CVE-2024-34470	0.932220000	0.997880000	<a href="#">Link</a>
CVE-2024-34102	0.943580000	0.999480000	<a href="#">Link</a>
CVE-2024-3400	0.942860000	0.999260000	<a href="#">Link</a>
CVE-2024-3273	0.944020000	0.999700000	<a href="#">Link</a>
CVE-2024-3272	0.937910000	0.998470000	<a href="#">Link</a>
CVE-2024-32651	0.913070000	0.996210000	<a href="#">Link</a>
CVE-2024-32113	0.934460000	0.998060000	<a href="#">Link</a>
CVE-2024-31982	0.941010000	0.998900000	<a href="#">Link</a>
CVE-2024-31851	0.914260000	0.996300000	<a href="#">Link</a>
CVE-2024-31850	0.909130000	0.995950000	<a href="#">Link</a>
CVE-2024-31849	0.919840000	0.996740000	<a href="#">Link</a>
CVE-2024-31848	0.927370000	0.997360000	<a href="#">Link</a>
CVE-2024-31750	0.926850000	0.997330000	<a href="#">Link</a>
CVE-2024-30255	0.921870000	0.996890000	<a href="#">Link</a>
CVE-2024-29973	0.936960000	0.998340000	<a href="#">Link</a>
CVE-2024-29972	0.915290000	0.996360000	<a href="#">Link</a>
CVE-2024-29895	0.930810000	0.997740000	<a href="#">Link</a>
CVE-2024-29824	0.943410000	0.999410000	<a href="#">Link</a>

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

Tue, 29 Apr 2025

**[NEU] [hoch] Redmine.org Redmine: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Redmine.org Redmine ausnutzen, um Informationen offenzulegen, einen Cross-Site Scripting Angriff durchzuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, einen Denial of Service Zustand auszulösen und mehrere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat FUSE ausnutzen, um vertrauliche Informationen offenzulegen, beliebigen Code auszuführen, einen Denial of Service Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Daten und Informationen zu manipulieren und seine Privilegien zu erweitern.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder nicht näher beschriebene Auswirkungen zu erzielen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und einen Spoofing-Angriff durchzuführen.

- [Link](#)

—

Tue, 29 Apr 2025

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

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

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen und um nicht näher beschriebene Auswirkungen zu erzielen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand oder andere, nicht näher beschriebene Auswirkungen zu verursachen.

- [Link](#)

—

Tue, 29 Apr 2025

**[UPDATE] [hoch] Apache Camel for Spring Boot: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Apache Camel, Red Hat Enterprise Linux und Red Hat Integration ausnutzen, um beliebigen Code auszuführen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um erhöhte Privilegi-

en zu erlangen oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Dateien zu manipulieren oder seine Rechte zu erweitern.

- [Link](#)

—

Tue, 29 Apr 2025

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung**

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, um beliebigen Programmcode auszuführen oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein entfernter Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Quarkus auf Red Hat Enterprise Linux ausnutzen, um Informationen offenzulegen, oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um nicht spezifizierte Auswirkungen zu erzeugen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen und um nicht näher beschriebene Auswirkungen zu verursachen.

- [Link](#)

---

Tue, 29 Apr 2025

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

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um erhöhte Rechte zu erlangen, beliebigen Code auszuführen, Spoofing-Angriffe durchzuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben oder andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

---

Tue, 29 Apr 2025

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

Ein entfernter anonymmer Angreifer kann mehrere Schwachstellen im Linux-Kernel ausnutzen, um einen 'Denial of Service'-Zustand zu erzeugen oder andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/29/2025	[FreeBSD : h11 accepts some malformed Chunked-Encoding bodies (df126e23-24fa-11f0-ab92-f02f7497ecda)]	critical
4/29/2025	[Google Chrome < 136.0.7103.48 Multiple Vulnerabilities]	critical
4/29/2025	[Google Chrome < 136.0.7103.48 Multiple Vulnerabilities]	critical
4/29/2025	[Amazon Linux 2 : firefox (ALASFIREFOX-2025-037)]	critical
4/29/2025	[Amazon Linux 2023 : firefox (ALAS2023-2025-943)]	high
4/29/2025	[Amazon Linux 2023 : java-17-amazon-corretto, java-17-amazon-corretto-devel, java-17-amazon-corretto-headless (ALAS2023-2025-954)]	high
4/29/2025	[Amazon Linux 2023 : java-24-amazon-corretto, java-24-amazon-corretto-devel, java-24-amazon-corretto-headless (ALAS2023-2025-951)]	high

Datum	Schwachstelle	Bewertung
4/29/2025	[Amazon Linux 2023 : bpftool, kernel6.12, kernel6.12-modules-extra (ALAS2023-2025-948)]	high
4/29/2025	[Amazon Linux 2023 : redis6, redis6-devel (ALAS2023-2025-950)]	high
4/29/2025	[Amazon Linux 2023 : java-11-amazon-corretto, java-11-amazon-corretto-devel, java-11-amazon-corretto-headless (ALAS2023-2025-955)]	high
4/29/2025	[Amazon Linux 2023 : libsoup, libsoup-devel (ALAS2023-2025-946)]	high
4/29/2025	[Amazon Linux 2023 : libsoup3, libsoup3-devel (ALAS2023-2025-941)]	high
4/29/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2025-090)]	high
4/29/2025	[Amazon Linux 2 : containerd (ALASECS-2025-060)]	high
4/29/2025	[Amazon Linux 2023 : bpftool, kernel6.12, kernel6.12-modules-extra (ALAS2023-2025-940)]	high
4/29/2025	[Amazon Linux 2 : java-11-openjdk (ALASJAVA-OPENJDK11-2025-011)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASECS-2025-062)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASECS-2025-059)]	high
4/29/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2025-100)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASECS-2025-058)]	high
4/29/2025	[Amazon Linux 2 : containerd (ALASDOCKER-2025-061)]	high
4/29/2025	[Amazon Linux 2 : runfinch-finch (ALASDOCKER-2025-057)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASDOCKER-2025-059)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASDOCKER-2025-060)]	high
4/29/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2025-070)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASNITRO-ENCLAVES-2025-055)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASECS-2025-064)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASECS-2025-061)]	high

Datum	Schwachstelle	Bewertung
4/29/2025	[Amazon Linux 2 : docker (ALASDOCKER-2025-058)]	high
4/29/2025	[Amazon Linux 2 : redis (ALASREDIS6-2025-012)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-059)]	high
4/29/2025	[Amazon Linux 2 : java-11-openjdk (ALASJAVA-OPENJDK11-2025-012)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-057)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-054)]	high
4/29/2025	[Amazon Linux 2 : containerd (ALASNITRO-ENCLAVES-2025-058)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASNITRO-ENCLAVES-2025-056)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASECS-2025-055)]	high
4/29/2025	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2025-119-02)]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

#### 4.0.1 Information Stealer. Wie funktionieren sie?



[Zum Youtube Video](#)



## 5 Cyberangriffe: (Mai)

Datum	Opfer	Land	Information
2025-05-09	Hessischen Apothekerverband	[DEU]	<a href="#">Link</a>
2025-05-06	West Lothian Council	[GBR]	<a href="#">Link</a>
2025-05-04	South African Airways	[ZAF]	<a href="#">Link</a>
2025-05-03	Coweta County School System	[USA]	<a href="#">Link</a>
2025-05-02	Outwood Academy Acklam	[GBR]	<a href="#">Link</a>
2025-05-01	Harrods	[GBR]	<a href="#">Link</a>
2025-05-01	Framlingham College	[GBR]	<a href="#">Link</a>
2025-05-01	Legal Aid Agency	[GBR]	<a href="#">Link</a>
2025-05-01	Breton S.p.A.	[ITA]	<a href="#">Link</a>

## 6 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-05-11	[www.regencytorviscas.com]	stormous	<a href="#">Link</a>
2025-05-11	[www.regencycountryclub.com]	stormous	<a href="#">Link</a>
2025-05-11	[www.regencyrestors.com]	stormous	<a href="#">Link</a>
2025-05-10	[Municipality of Pisa]	nova	<a href="#">Link</a>
2025-05-10	[Pienaar Brothers]	devman	<a href="#">Link</a>
2025-05-10	[Victim from Japan]	devman	<a href="#">Link</a>
2025-05-09	[EMX Enterprises]	play	<a href="#">Link</a>
2025-05-09	[Verrex]	play	<a href="#">Link</a>
2025-05-09	[Sweet Shop USA]	play	<a href="#">Link</a>
2025-05-09	[Gistic Research]	play	<a href="#">Link</a>
2025-05-06	[North Kitsap School District]	nightspire	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-05-08	[C.E.E. APTA]	nightspire	<a href="#">Link</a>
2025-05-09	[CHECKCITY.COM]	clop	<a href="#">Link</a>
2025-05-06	[Lake Shore Paving]	medusa	<a href="#">Link</a>
2025-05-06	[Russell Child Development Center]	medusa	<a href="#">Link</a>
2025-05-09	[Bervar and Jones]	akira	<a href="#">Link</a>
2025-05-09	[Klampfer Elektroanlagen]	akira	<a href="#">Link</a>
2025-05-09	[Mountain View Mushrooms]	rhysida	<a href="#">Link</a>
2025-05-09	[hennessyfund.com]	lockbit3	<a href="#">Link</a>
2025-05-09	[dailynews.co.th]	devman	<a href="#">Link</a>
2025-05-08	[101 Arch Street]	weyhro	<a href="#">Link</a>
2025-05-04	[SHRADERLAW]	qilin	<a href="#">Link</a>
2025-05-04	[www.hcsheriff.gov]	qilin	<a href="#">Link</a>
2025-05-08	[UniTrak]	play	<a href="#">Link</a>
2025-05-08	[Selenis (Evertis)]	akira	<a href="#">Link</a>
2025-05-08	[Selenis (Evertis is also involved)]	akira	<a href="#">Link</a>
2025-05-08	[novaevo+ / T.consult]	nova	<a href="#">Link</a>
2025-05-07	[Amtech Software]	monti	<a href="#">Link</a>
2025-05-08	[Khidmah]	everest	<a href="#">Link</a>
2025-05-08	[Kaefer]	everest	<a href="#">Link</a>
2025-05-07	[gmanetwork.com]	devman	<a href="#">Link</a>
2025-05-07	[Transport Lutzulln]	orca	<a href="#">Link</a>
2025-05-04	[Julia Evans accountants]	nightspire	<a href="#">Link</a>
2025-05-06	[mdgny.com]	qilin	<a href="#">Link</a>
2025-05-06	[clinpath.com]	qilin	<a href="#">Link</a>
2025-05-06	[jbanksdesign.com]	qilin	<a href="#">Link</a>
2025-05-06	[gates-cooper.com]	qilin	<a href="#">Link</a>
2025-05-06	[Langer & Langer]	SilentRansomGroup	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-05-06	[ehlers-inc.com]	lockbit3	<a href="#">Link</a>
2025-05-06	[eu-rec.de]	safepay	<a href="#">Link</a>
2025-05-06	[schapmann]	safepay	<a href="#">Link</a>
2025-05-06	[dosjm.com]	safepay	<a href="#">Link</a>
2025-05-06	[biglevel.net]	safepay	<a href="#">Link</a>
2025-05-06	[bloomfamilyeyesurgeons.com]	safepay	<a href="#">Link</a>
2025-05-06	[kolpa.com.pe]	safepay	<a href="#">Link</a>
2025-05-06	[dreng.com]	safepay	<a href="#">Link</a>
2025-05-06	[mooregiles.com]	safepay	<a href="#">Link</a>
2025-05-06	[Balance Diagnostics]	everest	<a href="#">Link</a>
2025-05-06	[Daniels & Taylor, P.C]	akira	<a href="#">Link</a>
2025-05-06	[NSS ██████████]	qilin	<a href="#">Link</a>
2025-05-05	[SNS SYSTEM]	killsec	<a href="#">Link</a>
2025-05-05	[Synthesia.com]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Grupo Herradura Occidente]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Croatianmint.hr]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Derp.org]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Abdainsurance.co.id]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Vnakc.org]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Goodson.com]	IMNCrew	<a href="#">Link</a>
2025-05-05	[Mediprobe Research]	rhysida	<a href="#">Link</a>
2025-05-05	[ATI Systems]	play	<a href="#">Link</a>
2025-05-05	[Novosit]	play	<a href="#">Link</a>
2025-05-05	[Downtown Travel]	play	<a href="#">Link</a>
2025-05-05	[Rand Technology]	play	<a href="#">Link</a>
2025-05-05	[Alberta Construction Safety Association]	play	<a href="#">Link</a>
2025-05-05	[Breen Construction Services]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-05-05	[Trybus]	play	<a href="#">Link</a>
2025-05-05	[Sugar Lake Lodge]	play	<a href="#">Link</a>
2025-05-05	[Marine Technical Surveyors]	play	<a href="#">Link</a>
2025-05-05	[Webcor]	play	<a href="#">Link</a>
2025-05-05	[Technical Die-Casting]	play	<a href="#">Link</a>
2025-05-05	[GPF Lewis]	hunters	<a href="#">Link</a>
2025-05-05	[Sioux Chief]	hunters	<a href="#">Link</a>
2025-05-05	[https://pestbusters.com.sg/]	devman	<a href="#">Link</a>
2025-05-05	[Pulmonary Physicians of South Florida Clinics]	BrainCipher	<a href="#">Link</a>
2025-05-05	[mbmdubai.com]	BrainCipher	<a href="#">Link</a>
2025-05-05	[ddecor.com]	BrainCipher	<a href="#">Link</a>
2025-05-05	[ruizre.es]	BrainCipher	<a href="#">Link</a>
2025-05-05	[soundtransit.org]	BrainCipher	<a href="#">Link</a>
2025-05-05	[valedolobo.com]	BrainCipher	<a href="#">Link</a>
2025-05-05	[edisoft.es]	BrainCipher	<a href="#">Link</a>
2025-05-05	[iycsa.com.co]	BrainCipher	<a href="#">Link</a>
2025-05-05	[Bentley Industries]	interlock	<a href="#">Link</a>
2025-05-04	[Cocoon]	silent	<a href="#">Link</a>
2025-05-04	[Lubiam]	sarcoma	<a href="#">Link</a>
2025-05-04	[NNC Firm]	sarcoma	<a href="#">Link</a>
2025-05-04	[Defiance]	sarcoma	<a href="#">Link</a>
2025-05-04	[Decoline]	sarcoma	<a href="#">Link</a>
2025-05-04	[TOMOKU CO., LTD.]	gunra	<a href="#">Link</a>
2025-05-03	[CabinC.com]	lynx	<a href="#">Link</a>
2025-05-03	[American Eagle Logistics]	monti	<a href="#">Link</a>
2025-05-03	[Kalin Hobeltechnik]	rhysida	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-05-03	[Fowler Elementary School]	interlock	<a href="#">Link</a>
2025-05-02	[HCI Informatique d'entreprise]	qilin	<a href="#">Link</a>
2025-05-02	[runtec.co.jp]	lynx	<a href="#">Link</a>
2025-05-01	[Jamjoom Pharma]	everest	<a href="#">Link</a>
2025-05-02	[derichsukonertz.de]	lynx	<a href="#">Link</a>
2025-05-02	[smvthailand.com]	devman	<a href="#">Link</a>
2025-05-01	[kll-law.com]	lockbit3	<a href="#">Link</a>
2025-05-01	[pdcn.com]	lockbit3	<a href="#">Link</a>
2025-05-01	[Government of Peru]	rhysida	<a href="#">Link</a>
2025-05-01	[Chinese Healthcare Organisation]	devman	<a href="#">Link</a>
2025-05-01	[Singapour Factory]	devman	<a href="#">Link</a>
2025-05-01	[Dedicated Web Consultants, Inc (USA) - dwcusa.com]	skira	<a href="#">Link</a>
2025-05-01	[www.newseason.com]	qilin	<a href="#">Link</a>
2025-05-01	[cobbcounty]	qilin	<a href="#">Link</a>
2025-05-01	[Defected Records]	play	<a href="#">Link</a>
2025-05-01	[ECOM America]	play	<a href="#">Link</a>
2025-05-01	[Southern Fidelity]	play	<a href="#">Link</a>
2025-05-01	[Custom Paper]	play	<a href="#">Link</a>
2025-05-01	[The Seydel Companies]	play	<a href="#">Link</a>
2025-05-01	[www.ancc.org]	qilin	<a href="#">Link</a>
2025-05-01	[Marsicovetere & Levine Law Group]	akira	<a href="#">Link</a>
2025-05-01	[Insight Pipe Contracting]	akira	<a href="#">Link</a>
2025-05-01	[StudioVaiani]	incransom	<a href="#">Link</a>
2025-05-01	[Weil Construction, Inc]	medusa	<a href="#">Link</a>
2025-05-01	[MALAYSIA AIRPORTS HOLDINGS BERHAD Part 1 of data taken !!!]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-05-01	[Janco Steel]	interlock	<a href="#">Link</a>
2025-05-01	[WDEF-TV]	lynx	<a href="#">Link</a>
2025-05-01	[South African IT firm]	devman	<a href="#">Link</a>
2025-05-01	[South African Hr company]	devman	<a href="#">Link</a>
2025-05-01	[dovesit.co.za]	devman	<a href="#">Link</a>

## 7 Quellen

### 7.1 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>

## 8 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.