

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240919



## 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>24</b>
5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection. . . . .	24
<b>6 Cyberangriffe: (Sep)</b>	<b>25</b>
<b>7 Ransomware-Erpressungen: (Sep)</b>	<b>26</b>
<b>8 Quellen</b>	<b>33</b>
8.1 Quellenverzeichnis . . . . .	33
<b>9 Impressum</b>	<b>35</b>

## 1 Editorial

Guten Morgen,

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

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

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

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

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

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

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

#### ***Sicherheitsupdates: BIOS-Lücken gefährden Dell-Computer***

Unter anderem sind bestimmte Computer von Dells Alienware-Serie attackierbar. Sicherheitspatches stehen zum Download.

- [Link](#)

—

#### ***Sicherheitslücken: Netzwerk-Controller und -Gateways von Aruba sind verwundbar***

Angreifer können Netzwerkgeräte von HPE Aruba attackieren und im schlimmsten Fall Appliances kompromittieren.

- [Link](#)

—

#### ***VMware vCenter: Angreifer aus dem Netz können Schadcode einschleusen***

Broadcom stopft mehrere Sicherheitslücken in VMware vCenter. Schlimmstenfalls können Angreifer aus dem Netz Schadcode einschmuggeln und ausführen.

- [Link](#)

—

#### ***Samsung-Druckertreiber ermöglichen Angreifern Rechteausweitung***

Für Samsungs Office-Drucker stellt HP einen aktualisierten Universal-Treiber für Windows bereit. Er dichtet ein Rechteausweitungsleck ab.

- [Link](#)

—

#### ***Angreifer attackieren Sicherheitslücken in Microsofts MSHTML und Whatsup Gold***

Die US-amerikanische IT-Sicherheitsbehörde CISA warnt vor Angriffen auf Sicherheitslücken in Microsofts MSHTML und Whatsup Gold.

- [Link](#)

—

#### ***Sicherheitspatch: Hintertür in einigen D-Link-Routern erlaubt unbefugte Zugriffe***

Angreifer können bestimmte Router-Modelle von D-Link attackieren und kompromittieren. Sicherheitsupdates stehen zum Download bereit.

- [Link](#)

—

#### ***Sicherheitspatch verfügbar: Angriffe auf Ivanti Cloud Service Appliance***

Derzeit attackieren Angreifer Ivanti Cloud Service Appliances mit Schadcode. Außerdem könnten Attacken auf Endpoint Manager bevorstehen.

- [Link](#)

---

**Lenovo schließt Lücken in BIOS, Management-Controller und WLAN-Treiber**

Wichtige Sicherheitsupdates schützen Computer von Lenovo. Im schlimmsten Fall können Angreifer Schadcode ausführen.

- [Link](#)

---

**Solarwinds ARM: Unbefugte Zugriffe und Schadcode-Attacken möglich**

Die Solarwinds-Entwickler haben zwei Sicherheitslücken in Access Rights Manager geschlossen. Eine Lücke gilt als kritisch.

- [Link](#)

---

**Sicherheitspatch: Gitlab behebt Lücken in Serverversionen**

Angreifer konnten Code einschleusen, fremde Konten übernehmen und den Server außer Gefecht setzen. Admins selbst gehosteter Instanzen sollten patchen.

- [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	0.957050000	0.994710000	<a href="#">Link</a>
CVE-2023-6895	0.921160000	0.990080000	<a href="#">Link</a>
CVE-2023-6553	0.947820000	0.993070000	<a href="#">Link</a>
CVE-2023-6019	0.918710000	0.989840000	<a href="#">Link</a>
CVE-2023-5360	0.902780000	0.988820000	<a href="#">Link</a>
CVE-2023-52251	0.945480000	0.992720000	<a href="#">Link</a>
CVE-2023-4966	0.970840000	0.998140000	<a href="#">Link</a>
CVE-2023-49103	0.949680000	0.993390000	<a href="#">Link</a>
CVE-2023-48795	0.965330000	0.996450000	<a href="#">Link</a>
CVE-2023-47246	0.961220000	0.995420000	<a href="#">Link</a>
CVE-2023-46805	0.950230000	0.993480000	<a href="#">Link</a>
CVE-2023-46747	0.971020000	0.998240000	<a href="#">Link</a>
CVE-2023-46604	0.969070000	0.997500000	<a href="#">Link</a>
CVE-2023-4542	0.948590000	0.993200000	<a href="#">Link</a>
CVE-2023-43208	0.973740000	0.999270000	<a href="#">Link</a>
CVE-2023-43177	0.961480000	0.995480000	<a href="#">Link</a>
CVE-2023-42793	0.972380000	0.998690000	<a href="#">Link</a>
CVE-2023-41265	0.907590000	0.989100000	<a href="#">Link</a>
CVE-2023-39143	0.940700000	0.992170000	<a href="#">Link</a>
CVE-2023-38205	0.950330000	0.993490000	<a href="#">Link</a>
CVE-2023-38203	0.965830000	0.996580000	<a href="#">Link</a>
CVE-2023-38146	0.919150000	0.989880000	<a href="#">Link</a>
CVE-2023-38035	0.974690000	0.999720000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967850000	0.997120000	<a href="#">Link</a>
CVE-2023-3519	0.965910000	0.996600000	<a href="#">Link</a>
CVE-2023-35082	0.966710000	0.996810000	<a href="#">Link</a>
CVE-2023-35078	0.970930000	0.998180000	<a href="#">Link</a>
CVE-2023-34993	0.973450000	0.999170000	<a href="#">Link</a>
CVE-2023-34960	0.900520000	0.988650000	<a href="#">Link</a>
CVE-2023-34634	0.923140000	0.990260000	<a href="#">Link</a>
CVE-2023-34362	0.970450000	0.997970000	<a href="#">Link</a>
CVE-2023-34039	0.945100000	0.992670000	<a href="#">Link</a>
CVE-2023-3368	0.939780000	0.992060000	<a href="#">Link</a>
CVE-2023-33246	0.967830000	0.997120000	<a href="#">Link</a>
CVE-2023-32315	0.971490000	0.998400000	<a href="#">Link</a>
CVE-2023-30625	0.953610000	0.994110000	<a href="#">Link</a>
CVE-2023-30013	0.965950000	0.996610000	<a href="#">Link</a>
CVE-2023-29300	0.969240000	0.997540000	<a href="#">Link</a>
CVE-2023-29298	0.970810000	0.998110000	<a href="#">Link</a>
CVE-2023-28432	0.920500000	0.990020000	<a href="#">Link</a>
CVE-2023-28343	0.933130000	0.991330000	<a href="#">Link</a>
CVE-2023-28121	0.925430000	0.990500000	<a href="#">Link</a>
CVE-2023-27524	0.970600000	0.998010000	<a href="#">Link</a>
CVE-2023-27372	0.973930000	0.999350000	<a href="#">Link</a>
CVE-2023-27350	0.969520000	0.997620000	<a href="#">Link</a>
CVE-2023-26469	0.953540000	0.994080000	<a href="#">Link</a>
CVE-2023-26360	0.964390000	0.996130000	<a href="#">Link</a>
CVE-2023-26035	0.968720000	0.997380000	<a href="#">Link</a>
CVE-2023-25717	0.954660000	0.994280000	<a href="#">Link</a>
CVE-2023-25194	0.965150000	0.996360000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963230000	0.995830000	<a href="#">Link</a>
CVE-2023-24489	0.973150000	0.999050000	<a href="#">Link</a>
CVE-2023-23752	0.951460000	0.993660000	<a href="#">Link</a>
CVE-2023-23333	0.960430000	0.995230000	<a href="#">Link</a>
CVE-2023-22527	0.970940000	0.998200000	<a href="#">Link</a>
CVE-2023-22518	0.961800000	0.995550000	<a href="#">Link</a>
CVE-2023-22515	0.973160000	0.999070000	<a href="#">Link</a>
CVE-2023-21839	0.951270000	0.993620000	<a href="#">Link</a>
CVE-2023-21554	0.955880000	0.994500000	<a href="#">Link</a>
CVE-2023-20887	0.970840000	0.998140000	<a href="#">Link</a>
CVE-2023-1671	0.962220000	0.995630000	<a href="#">Link</a>
CVE-2023-0669	0.971300000	0.998350000	<a href="#">Link</a>

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

Wed, 18 Sep 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](#)

—

Wed, 18 Sep 2024

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

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

- [Link](#)

—



Wed, 18 Sep 2024

**[NEU] [hoch] Red Hat OpenShift: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 18 Sep 2024

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

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

- [Link](#)

—

Wed, 18 Sep 2024

**[NEU] [hoch] Microsoft Dynamics 365: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Microsoft Dynamics 365 ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 18 Sep 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](#)

—

Wed, 18 Sep 2024

**[NEU] [hoch] GitLab: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in GitLab und Ruby ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Wed, 18 Sep 2024

**[UPDATE] [hoch] TLS: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in TLS 1.2 ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—  
Wed, 18 Sep 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 18 Sep 2024

**[UPDATE] [hoch] Dell PowerEdge: Schwachstelle ermöglicht Erlangen von Administratorrechten**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Dell PowerEdge ausnutzen, um Administratorrechte zu erlangen.

- [Link](#)

—

Wed, 18 Sep 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 18 Sep 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](#)

—

Wed, 18 Sep 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in GStreamer ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 18 Sep 2024

**[UPDATE] [hoch] Ghostscript: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ghostscript ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- [Link](#)

—

Wed, 18 Sep 2024

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

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

- [Link](#)

—

Wed, 18 Sep 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](#)

—

Wed, 18 Sep 2024

**[UPDATE] [kritisch] FRRouting Project FRRouting: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FRRouting Project FRRouting ausnutzen, um einen Denial of Service Zustand zu erzeugen und potenziell beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 18 Sep 2024

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

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

- [Link](#)

—

Wed, 18 Sep 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 beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen oder Daten zu manipulieren.

- [Link](#)

—

Tue, 17 Sep 2024

**[UPDATE] [kritisch] Ivanti Endpoint Manager: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Ivanti Endpoint Manager ausnutzen, um beliebigen

Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, erweiterte Rechte zu erlangen und vertrauliche Informationen preiszugeben.

- [Link](#)

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
9/18/2024	[Ubuntu 14.04 LTS : OpenSSL vulnerabilities (USN-7018-1)]	critical
9/18/2024	[Photon OS 3.0: Expat PHSA-2024-3.0-0796]	critical
9/18/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Apache HTTP Server vulnerabilities (USN-6885-3)]	critical
9/18/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-7019-1)]	critical
9/18/2024	[SolarWinds ARM 2024.3.1 Multiple Vulnerabilities (2024-3-1)]	critical
9/18/2024	[RHEL 9 : expat (RHSA-2024:6754)]	critical
9/18/2024	[Ivanti Endpoint Manager 2022 - September Security Update]	critical
9/18/2024	[Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel vulnerabilities (USN-7020-1)]	critical
9/18/2024	[RHEL 8 / 9 : Red Hat Ansible Automation Platform 2.4 Product Security and Bug Fix Update (Moderate) (RHSA-2024:6765)]	critical
9/18/2024	[Debian dla-3892 : tinyproxy - security update]	critical
9/18/2024	[Amazon Linux 2 : firefox (ALASFIREFOX-2024-029)]	critical
9/18/2024	[Amazon Linux 2 : firefox (ALASFIREFOX-2024-030)]	critical
9/18/2024	[Amazon Linux 2 : openssl-snapsafe (ALASOPENSSL-SNAPSAFE-2024-006)]	critical

Datum	Schwachstelle	Bewertung
9/17/2024	[Debian dsa-5770 : expat - security update]	critical
9/18/2024	[openSUSE 15 Security Update : gstreamer-plugins-bad (openSUSE-SU-2024:0305-1)]	high
9/18/2024	[FreeBSD : OpenSSH – Pre-authentication async signal safety issue (58750d49-7302-11ef-8c95-195d300202b3)]	high
9/18/2024	[Fedora 39 : chromium (2024-37f95ce86b)]	high
9/18/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gstreamer-plugins-bad, libvpl (SUSE-SU-2024:3289-1)]	high
9/18/2024	[Oracle Linux 9 : fence-agents (ELSA-2024-6726)]	high
9/18/2024	[Spring Framework < 5.3.40 / 6.0.x < 6.0.24 / 6.1.x < 6.1.13 Path Traversal (CVE-2024-38816)]	high
9/18/2024	[RHEL 8 : kernel (RHSA-2024:6753)]	high
9/18/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-7021-1)]	high
9/18/2024	[RHEL 9 : libnbd (RHSA-2024:6757)]	high
9/18/2024	[Oracle Linux 7 : kernel (ELSA-2024-5259)]	high
9/18/2024	[Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-7022-1)]	high
9/18/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-084)]	high
9/18/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-053)]	high
9/18/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-085)]	high
9/18/2024	[Amazon Linux 2 : microcode_ctl (ALAS-2024-2635)]	high
9/18/2024	[Amazon Linux 2 : ruby (ALAS-2024-2637)]	high
9/18/2024	[Amazon Linux 2 : python2-setuptools (ALAS-2024-2632)]	high
9/17/2024	[Google Chrome < 129.0.6668.58 Multiple Vulnerabilities]	high
9/17/2024	[Google Chrome < 129.0.6668.58 Multiple Vulnerabilities]	high
9/17/2024	[Debian dsa-5772 : fonts-opensymbol - security update]	high
9/17/2024	[Debian dsa-5771 : php-twig - security update]	high
9/17/2024	[Amazon Linux AMI : microcode_ctl (ALAS-2024-1946)]	high

Datum	Schwachstelle	Bewertung
9/17/2024	[Oracle Linux 7 : java-1.8.0-openjdk (ELSA-2024-4560)]	high
9/17/2024	[Oracle Linux 7 : ghostscript (ELSA-2024-4549)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Wed, 18 Sep 2024

#### **Online Traffic Offense 1.0 CSRF / Arbitrary File Upload**

Online Traffic Offense version 1.0 suffers from cross site request forgery and arbitrary file upload vulnerabilities.

- [Link](#)

—

” “Wed, 18 Sep 2024

#### **Backdoor.Win32.CCInvader.10 MVID-2024-0694 Authentication Bypass**

Backdoor.Win32.CCInvader.10 malware suffers from a bypass vulnerability.

- [Link](#)

—

” “Wed, 18 Sep 2024

#### **Backdoor.Win32.BlackAngel.13 MVID-2024-0695 Code Execution**

Backdoor.Win32.BlackAngel.13 malware suffers from a code execution vulnerability.

- [Link](#)

—

” “Wed, 18 Sep 2024

#### **Backdoor.Win32.Delf.yj MVID-2024-0693 Information Disclosure**

Backdoor.Win32.Delf.yj malware suffers from an information leakage vulnerability.

- [Link](#)

—

” “Wed, 18 Sep 2024

#### **Online Exam System 1.0 Insecure Settings**

Online Exam System version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Wed, 18 Sep 2024

**Online Bus Ticket Booking Website 1.0 SQL Injection**

Online Bus Ticket Booking Website version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Wed, 18 Sep 2024

**Nipah Virus Testing Management System 1.0 SQL Injection**

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

- [Link](#)

—

” “Wed, 18 Sep 2024

**Membership Management System 1.1 SQL Injection**

Membership Management System version 1.1 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Wed, 18 Sep 2024

**HYSICAL System 1.9 Add Administrator / Cross Site Request Forgery**

HYSICAL System version 1.9 suffers from add administrator and cross site request forgery vulnerabilities.

- [Link](#)

—

” “Wed, 18 Sep 2024

**Furniture Master 2 SQL Injection**

Furniture Master version 2 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Wed, 18 Sep 2024

**Food Ordering And Table Reservation System For Restaurants 1.0 Insecure Settings**

Food Ordering and Table Reservation System for Restaurants version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Wed, 18 Sep 2024

**Beauty Parlour And Saloon Management System 1.1 Insecure Settings**

Beauty Parlour and Saloon Management System version 1.1 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024

***Microsoft Windows TOCTOU Local Privilege Escalation***

CVE-2024-30088 is a Windows kernel elevation of privilege vulnerability which affects many recent versions of Windows 10, Windows 11 and Windows Server 2022. The vulnerability exists inside the function called AuthzBasepCopyoutInternalSecurityAttributes specifically when the kernel copies the \_AUTHZBASEP\_SECURITY\_ATTRIBUTES\_INFORMATION of the current token object to user mode. When the kernel performs the copy of the SecurityAttributesList, it sets up the list of the SecurityAttributes structure directly to the user supplied pointed. It then calls RtlCopyUnicodeString and AuthzBasepCopyoutInternalSecurityAttributeValues to copy out the names and values of the SecurityAttribute leading to multiple Time Of Check Time Of Use (TOCTOU) vulnerabilities in the function.

- [Link](#)

—

” “Tue, 17 Sep 2024

***WordPress LiteSpeed Cache Cookie Theft***

This Metasploit module exploits an unauthenticated account takeover vulnerability in LiteSpeed Cache, a WordPress plugin that currently has around 6 million active installations. In LiteSpeed Cache versions prior to 6.5.0.1, when the Debug Logging feature is enabled, the plugin will log admin cookies to the /wp-content/debug.log endpoint which is accessible without authentication. The Debug Logging feature in the plugin is not enabled by default. The admin cookies found in the debug.log can be used to upload and execute a malicious plugin containing a payload.

- [Link](#)

—

” “Tue, 17 Sep 2024

***GibbonEdu Core 26.0.00 Cross Site Scripting***

GibbonEdu Core version 26.0.00 suffers from a cross site scripting vulnerability that can lead to privilege escalation.

- [Link](#)

—

” “Tue, 17 Sep 2024

***TP-Link Archer AX50 Cross Site Scripting***

TP-Link Archer AX50 router with firmware version 1.0.11 build 2022052 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024



**HTMLy 2.9.9 Cross Site Scripting**

HTMLy version 2.9.9 suffers from a persistent cross site scripting vulnerability that can lead to account takeover.

- [Link](#)

—

” “Tue, 17 Sep 2024

**Dockwatch Remote Command Execution**

Dockwatch is a container management web UI for docker. It runs by default without authentication, although guidance is available for how to setup credentials for access. It has a Commands feature that allows a user to run docker commands such as inspect, network, ps. Prior to fix, it did not restrict input for parameters, so both container and parameters for the dockerInspect command were vulnerable to shell command injection on the container as the abc user with (limited) command output. See commits 23df366 and c091e4c for fixes.

- [Link](#)

—

” “Tue, 17 Sep 2024

**Microsoft SQL Server Masked Data Exposure**

Microsoft SQL Server versions 2014, 2016, 2017, 2019, and 2022 suffer from an issue where masked data can be exposed through a brute force attack.

- [Link](#)

—

” “Tue, 17 Sep 2024

**SPIP BigUp 4.0 Code Injection**

SPIP BigUp version 4.0 suffers from a remote PHP code injection vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024

**Online Student Grading System 1.0 Code Injection**

Online Student Grading System version 1.0 suffers from a remote PHP code injection vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024

**Online Notice Board System 1.0 Arbitrary File Upload**

Online Notice Board System version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024

**Online Bus Ticket Booking Website 1.0 Arbitrary File Upload**

Online Bus Ticket Booking Website version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024

***Old Age Home Management System 1.0 Code Injection***

Old Age Home Management System version 1.0 suffers from a remote PHP code injection vulnerability.

- [Link](#)

—

” “Tue, 17 Sep 2024

***Membership Management System 1.0 Code Injection***

Membership Management System version 1.0 suffers from a remote PHP code injection vulnerability.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Tue, 17 Sep 2024

***ZDI-24-1272: PDF-XChange Editor AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1271: PDF-XChange Editor AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1270: PDF-XChange Editor Doc Object Out-Of-Bounds Read Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1269: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1268: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1267: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1266: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1265: PDF-XChange Editor RTF File Parsing Uninitialized Variable Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1264: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1263: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1262: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1261: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1260: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1259: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1258: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1257: PDF-XChange Editor TIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1256: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1255: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

***ZDI-24-1254: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1253: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1252: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1251: PDF-XChange Editor EMF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1250: PDF-XChange Editor PPM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1249: PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1248: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1247: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1246: PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1245: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1244: PDF-XChange Editor U3D File Parsing Use-After-Free Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1243: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1242: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1241: PDF-XChange Editor U3D File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1240: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1239: PDF-XChange Editor U3D File Parsing Use-After-Free Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1238: PDF-XChange Editor U3D File Parsing Memory Corruption Remote Code Execution**

**Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1237: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution**

**Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1236: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution**

**Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1235: PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Remote Code Execution**

**Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1234: WinZip Mark-of-the-Web Bypass Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1233: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1232: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1231: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1230: Cohesive Networks VNS3 Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1229: BlueZ HID over GATT Profile Improper Access Control Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1228: Trend Micro Deep Discovery Inspector SQL Injection Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 17 Sep 2024

**ZDI-24-1227: Trend Micro Deep Discovery Inspector SQL Injection Information Disclosure Vulnerability**

- [Link](#)

—

”



## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 X-Correlation-Id: An der Flughafen-Security vorbei mit SQL-Injection.



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Sep)

Datum	Opfer	Land	Information
2024-09-16	TAAG	[AGO]	<a href="#">Link</a>
2024-09-16	Heinrich-Böll-Gesamtschule et Rurtal-Gymnasium	[DEU]	<a href="#">Link</a>
2024-09-16	Fylde Coast Academy Trust	[GBR]	<a href="#">Link</a>
2024-09-15	Radio Geretsried	[DEU]	<a href="#">Link</a>
2024-09-14	Zacros	[JPN]	<a href="#">Link</a>
2024-09-12	東京都庁 (Kantsu)	[JPN]	<a href="#">Link</a>
2024-09-12	LolaLiza	[BEL]	<a href="#">Link</a>
2024-09-09	Université de Gênes	[ITA]	<a href="#">Link</a>
2024-09-08	Highline Public Schools	[USA]	<a href="#">Link</a>
2024-09-08	Groupe Bayard	[FRA]	<a href="#">Link</a>
2024-09-08	Isbergues	[FRA]	<a href="#">Link</a>
2024-09-06	Superior Tribunal de Justiça (STJ)	[BRA]	<a href="#">Link</a>
2024-09-05	Air-e	[COL]	<a href="#">Link</a>
2024-09-05	Charles Darwin School	[GBR]	<a href="#">Link</a>
2024-09-05	Elektroskandia	[SWE]	<a href="#">Link</a>
2024-09-04	Tewkesbury Borough Council	[GBR]	<a href="#">Link</a>
2024-09-04	Swire Pacific Offshore (SPO)	[SGP]	<a href="#">Link</a>
2024-09-04	Compass Group	[AUS]	<a href="#">Link</a>
2024-09-02	Transport for London (TfL)	[GBR]	<a href="#">Link</a>
2024-09-02	Conseil national de l'ordre des experts-comptables (CNOEC)	[FRA]	<a href="#">Link</a>
2024-09-02	Kawasaki Motors Europe	[GBR]	<a href="#">Link</a>
2024-09-01	Wertachkliniken	[DEU]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Sep)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-18	[Handala's statement]	handala	<a href="#">Link</a>
2024-09-18	[bspcr.com]	lockbit3	<a href="#">Link</a>
2024-09-18	[lakelandchamber.com]	lockbit3	<a href="#">Link</a>
2024-09-18	[yesmoke.eu]	lockbit3	<a href="#">Link</a>
2024-09-18	[efile.com]	lockbit3	<a href="#">Link</a>
2024-09-18	[paybito.com]	lockbit3	<a href="#">Link</a>
2024-09-18	[Compass Group (2nd attack)]	medusa	<a href="#">Link</a>
2024-09-18	[Structural Concepts]	medusa	<a href="#">Link</a>
2024-09-19	[Vidisco]	handala	<a href="#">Link</a>
2024-09-19	[IIB ( Israeli Industrial Batteries )]	handala	<a href="#">Link</a>
2024-09-18	[Plaisted Companies]	play	<a href="#">Link</a>
2024-09-11	[Bertelkamp Automation]	qilin	<a href="#">Link</a>
2024-09-18	[DJH Jugendherberge]	hunters	<a href="#">Link</a>
2024-09-18	[Prentke Romich Company]	fog	<a href="#">Link</a>
2024-09-12	[agricola]	qilin	<a href="#">Link</a>
2024-09-16	[Amerinational Community Services]	medusa	<a href="#">Link</a>
2024-09-16	[Providence Public School Department]	medusa	<a href="#">Link</a>
2024-09-16	[AZPIRED]	medusa	<a href="#">Link</a>
2024-09-17	[Compass Group]	medusa	<a href="#">Link</a>
2024-09-18	[Chernan Technology]	orca	<a href="#">Link</a>
2024-09-18	[Port of Seattle/Seattle-Tacoma International Airport (SEA)]	rhysida	<a href="#">Link</a>
2024-09-16	[Baskervill]	play	<a href="#">Link</a>
2024-09-16	[Protective Industrial Products]	play	<a href="#">Link</a>
2024-09-16	[Inktel]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-16	[Rsp]	play	<a href="#">Link</a>
2024-09-16	[Hariri Pontarini Architects]	play	<a href="#">Link</a>
2024-09-16	[Multidata]	play	<a href="#">Link</a>
2024-09-18	[Environmental Code Consultants Inc]	meow	<a href="#">Link</a>
2024-09-18	[EnviroNET Inc]	meow	<a href="#">Link</a>
2024-09-18	[Robson Planning Group Inc]	meow	<a href="#">Link</a>
2024-09-16	[oipip.gda.pl]	ransomhub	<a href="#">Link</a>
2024-09-16	[kryptonresources.com]	ransomhub	<a href="#">Link</a>
2024-09-16	[www.tta.cls]	ransomhub	<a href="#">Link</a>
2024-09-18	[globe.com.bd]	ValenciaLeaks	<a href="#">Link</a>
2024-09-18	[satiagroup.com]	ValenciaLeaks	<a href="#">Link</a>
2024-09-18	[duopharmabiotech.com]	ValenciaLeaks	<a href="#">Link</a>
2024-09-18	[tendam.es]	ValenciaLeaks	<a href="#">Link</a>
2024-09-18	[cityofpleasantonca.gov]	ValenciaLeaks	<a href="#">Link</a>
2024-09-16	[www.faithfc.org]	ransomhub	<a href="#">Link</a>
2024-09-16	[www.adantia.es]	ransomhub	<a href="#">Link</a>
2024-09-16	[topdoctors.com]	ransomhub	<a href="#">Link</a>
2024-09-16	[www.8010urbanliving.com]	ransomhub	<a href="#">Link</a>
2024-09-16	[www.taperuvicha.com]	ransomhub	<a href="#">Link</a>
2024-09-17	[www.plumbersstock.com]	ransomhub	<a href="#">Link</a>
2024-09-17	[www.nikpol.com.au]	ransomhub	<a href="#">Link</a>
2024-09-18	[www.galloway-macleod.co.uk]	ransomhub	<a href="#">Link</a>
2024-09-18	[ringpower.com]	ransomhub	<a href="#">Link</a>
2024-09-17	[miit.gov.cn]	killsec	<a href="#">Link</a>
2024-09-17	[New Electric]	hunters	<a href="#">Link</a>
2024-09-17	[AutoCanada]	hunters	<a href="#">Link</a>
2024-09-17	[natcoglobal.com]	cactus	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-17	[Sherr Puttmann Akins Lamb PC]	bianlian	<a href="#">Link</a>
2024-09-17	[peerlessumbrella.com]	cactus	<a href="#">Link</a>
2024-09-17	[thomas-lloyd.com]	cactus	<a href="#">Link</a>
2024-09-16	[Cruz Marine (cruz.local)]	lynx	<a href="#">Link</a>
2024-09-16	[SuperCommerce.ai]	killsec	<a href="#">Link</a>
2024-09-16	[MCNA Dental 1 million patients records]	everest	<a href="#">Link</a>
2024-09-16	[ExcelPlast Tunisie]	orca	<a href="#">Link</a>
2024-09-16	[northernsafety.com]	blackbasta	<a href="#">Link</a>
2024-09-16	[thompsoncreek.com]	blackbasta	<a href="#">Link</a>
2024-09-07	[www.atlcc.net]	ransomhub	<a href="#">Link</a>
2024-09-10	[accuraterailroad.com]	ransomhub	<a href="#">Link</a>
2024-09-10	[advantagecdc.org]	ransomhub	<a href="#">Link</a>
2024-09-10	[lafuturasrl.it]	ransomhub	<a href="#">Link</a>
2024-09-15	[dowley.com]	lockbit3	<a href="#">Link</a>
2024-09-15	[apexbrasil.com.br]	lockbit3	<a href="#">Link</a>
2024-09-15	[fivestarproducts.com]	lockbit3	<a href="#">Link</a>
2024-09-15	[ignitarium.com]	lockbit3	<a href="#">Link</a>
2024-09-15	[nfcaa.org]	lockbit3	<a href="#">Link</a>
2024-09-15	[Emtel]	arcusmedia	<a href="#">Link</a>
2024-09-15	[EAGLE School]	qilin	<a href="#">Link</a>
2024-09-15	[salaam.af]	lockbit3	<a href="#">Link</a>
2024-09-15	[INTERNAL.ROCKYMOUNTAINGASTRO.COM]	trinity	<a href="#">Link</a>
2024-09-14	[Gino Giglio Generation Spa]	arcusmedia	<a href="#">Link</a>
2024-09-14	[Rextech]	arcusmedia	<a href="#">Link</a>
2024-09-14	[Like Family's]	arcusmedia	<a href="#">Link</a>
2024-09-14	[UNI-PA A.Ş.]	arcusmedia	<a href="#">Link</a>
2024-09-12	[OnePoint Patient Care]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-14	[Retemex]	ransomexx	<a href="#">Link</a>
2024-09-14	[ORCHID-ORTHO.COM]	clop	<a href="#">Link</a>
2024-09-11	[jatelindo]	stormous	<a href="#">Link</a>
2024-09-13	[mivideo.club]	stormous	<a href="#">Link</a>
2024-09-12	[Micron Internet]	medusa	<a href="#">Link</a>
2024-09-12	[TECHNOLOG S.r.l.]	medusa	<a href="#">Link</a>
2024-09-14	[ecbawm.com]	abyss	<a href="#">Link</a>
2024-09-13	[FD Lawrence Electric]	blacksuit	<a href="#">Link</a>
2024-09-13	[True Family Enterprises]	play	<a href="#">Link</a>
2024-09-13	[Dimensional Merchandising]	play	<a href="#">Link</a>
2024-09-13	[Creative Playthings]	play	<a href="#">Link</a>
2024-09-13	[Law Offices of Michael J Gurfinkel, Inc]	bianlian	<a href="#">Link</a>
2024-09-13	[Hostetler Buildings]	blacksuit	<a href="#">Link</a>
2024-09-13	[Vicom Corporation]	hunters	<a href="#">Link</a>
2024-09-13	[Arch-Con]	hunters	<a href="#">Link</a>
2024-09-13	[HB Construction]	hunters	<a href="#">Link</a>
2024-09-13	[Associated Building Specialties]	hunters	<a href="#">Link</a>
2024-09-12	[www.southeasternretina.com]	ransomhub	<a href="#">Link</a>
2024-09-11	[Ascend Analytics (ascendanalytics.com)]	lynx	<a href="#">Link</a>
2024-09-06	[Kingsmill Resort]	qilin	<a href="#">Link</a>
2024-09-12	[brunswickhospitalcenter.org]	threeam	<a href="#">Link</a>
2024-09-12	[Carpenter McCadden and Lane LLP]	meow	<a href="#">Link</a>
2024-09-12	[CSMR Agrupación de Colaboración Empresaria]	meow	<a href="#">Link</a>
2024-09-11	[ICBC (London)]	hunters	<a href="#">Link</a>
2024-09-12	[thornton-inc.com]	ransomhub	<a href="#">Link</a>
2024-09-04	[nhbg.com.co]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-12	[mechdyne.com]	ransomhub	<a href="#">Link</a>
2024-09-10	[Starr-Iva Water & Sewer District]	medusa	<a href="#">Link</a>
2024-09-10	[Karakaya Group]	medusa	<a href="#">Link</a>
2024-09-10	[allamericanpoly.com]	ransomhub	<a href="#">Link</a>
2024-09-11	[Charles Darwin School]	blacksuit	<a href="#">Link</a>
2024-09-11	[S. Walter Packaging]	fog	<a href="#">Link</a>
2024-09-11	[Clatronic International GmbH]	fog	<a href="#">Link</a>
2024-09-11	[Advanced Physician Management Services LLC]	meow	<a href="#">Link</a>
2024-09-11	[Arville]	meow	<a href="#">Link</a>
2024-09-11	[ICBC London]	hunters	<a href="#">Link</a>
2024-09-11	[Ladov Law Firm]	bianlian	<a href="#">Link</a>
2024-09-10	[Regent Care Center]	incransom	<a href="#">Link</a>
2024-09-10	[www.vinatiorganics.com]	ransomhub	<a href="#">Link</a>
2024-09-10	[Evans Distribution Systems]	play	<a href="#">Link</a>
2024-09-10	[Weldco-Beales Manufacturing]	play	<a href="#">Link</a>
2024-09-10	[PIGGLY WIGGLY ALABAMA DISTRIBUTING]	play	<a href="#">Link</a>
2024-09-10	[Elgin Separation Solutions]	play	<a href="#">Link</a>
2024-09-10	[Bel-Air Bay Club]	play	<a href="#">Link</a>
2024-09-10	[Joe Swartz Electric]	play	<a href="#">Link</a>
2024-09-10	[Virginia Dare Extract Co.]	play	<a href="#">Link</a>
2024-09-10	[Southeast Cooler]	play	<a href="#">Link</a>
2024-09-10	[IDF and Mossad agents]	meow	<a href="#">Link</a>
2024-09-10	[rupicard.com]	killsec	<a href="#">Link</a>
2024-09-10	[Vickers Engineering]	akira	<a href="#">Link</a>
2024-09-09	[Controlled Power]	dragonforce	<a href="#">Link</a>
2024-09-09	[Arc-Com]	dragonforce	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-10	[HDI]	bianlian	<a href="#">Link</a>
2024-09-10	[Myelec Electrical]	meow	<a href="#">Link</a>
2024-09-10	[Kadokawa Co Jp]	blacksuit	<a href="#">Link</a>
2024-09-10	[Qeco/coeq]	rhysida	<a href="#">Link</a>
2024-09-10	[E-Z Pack Holdings LLC]	incransom	<a href="#">Link</a>
2024-09-10	[Bank Rakyat]	hunters	<a href="#">Link</a>
2024-09-06	[americagraphics.com]	ransomhub	<a href="#">Link</a>
2024-09-09	[Pennsylvania State Education Association]	rhysida	<a href="#">Link</a>
2024-09-09	[Anniversary Holding]	bianlian	<a href="#">Link</a>
2024-09-09	[Battle Lumber Co.]	bianlian	<a href="#">Link</a>
2024-09-09	[www.unige.it]	ransomhub	<a href="#">Link</a>
2024-09-09	[Appellation vins fins]	ransomhub	<a href="#">Link</a>
2024-09-07	[www.dpe.go.th]	ransomhub	<a href="#">Link</a>
2024-09-09	[www.bsg.com.au]	ransomhub	<a href="#">Link</a>
2024-09-09	[schynsassurances.be]	killsec	<a href="#">Link</a>
2024-09-09	[pv.be]	killsec	<a href="#">Link</a>
2024-09-09	[Smart Source, Inc.]	bianlian	<a href="#">Link</a>
2024-09-08	[CAM Tyre Trade Systems & Solutions]	qilin	<a href="#">Link</a>
2024-09-06	[XXXXXXXXXX]	cicada3301	<a href="#">Link</a>
2024-09-08	[Stratford School Academy]	rhysida	<a href="#">Link</a>
2024-09-07	[Prosolit]	medusa	<a href="#">Link</a>
2024-09-07	[Grupo Cortefiel]	medusa	<a href="#">Link</a>
2024-09-07	[Nocciole Marchisio]	meow	<a href="#">Link</a>
2024-09-07	[Elsoms Seeds]	meow	<a href="#">Link</a>
2024-09-07	[Millsboro Animal Hospital]	qilin	<a href="#">Link</a>
2024-09-05	[briedis.lt]	ransomhub	<a href="#">Link</a>
2024-09-06	[America Voice]	medusa	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-06	[CK Associates]	bianlian	<a href="#">Link</a>
2024-09-06	[Keya Accounting and Tax Services LLC]	bianlian	<a href="#">Link</a>
2024-09-06	[ctelift.com]	madliberator	<a href="#">Link</a>
2024-09-06	[SESAM Informatics]	hunters	<a href="#">Link</a>
2024-09-06	[riomarineinc.com]	cactus	<a href="#">Link</a>
2024-09-06	[champeau.com]	cactus	<a href="#">Link</a>
2024-09-05	[cda.be]	killsec	<a href="#">Link</a>
2024-09-05	[belfius.be]	killsec	<a href="#">Link</a>
2024-09-05	[dvv.be]	killsec	<a href="#">Link</a>
2024-09-05	[Custom Security Systems]	hunters	<a href="#">Link</a>
2024-09-05	[Inglenorth.co.uk]	ransomhub	<a href="#">Link</a>
2024-09-05	[cps-k12.org]	ransomhub	<a href="#">Link</a>
2024-09-05	[inorde.com]	ransomhub	<a href="#">Link</a>
2024-09-05	[PhD Services]	dragonforce	<a href="#">Link</a>
2024-09-05	[kawasaki.eu]	ransomhub	<a href="#">Link</a>
2024-09-01	[cbt-gmbh.de]	ransomhub	<a href="#">Link</a>
2024-09-05	[www.towellengineering.net]	ransomhub	<a href="#">Link</a>
2024-09-04	[rhp.com.br]	lockbit3	<a href="#">Link</a>
2024-09-05	[Baird Mandalas Brockstedt LLC]	akira	<a href="#">Link</a>
2024-09-05	[Imetame]	akira	<a href="#">Link</a>
2024-09-05	[SWISS CZ]	akira	<a href="#">Link</a>
2024-09-05	[Cellular Plus]	akira	<a href="#">Link</a>
2024-09-05	[Arch Street Capital Advisors]	qilin	<a href="#">Link</a>
2024-09-04	[Hospital Episcopal San Lucas]	medusa	<a href="#">Link</a>
2024-09-05	[www.parknfly.ca]	ransomhub	<a href="#">Link</a>
2024-09-05	[Western Supplies, Inc]	bianlian	<a href="#">Link</a>
2024-09-04	[Farmers' Rice Cooperative]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-09-04	[Bakersfield]	play	<a href="#">Link</a>
2024-09-04	[Crain Group]	play	<a href="#">Link</a>
2024-09-04	[Parrish]	blacksuit	<a href="#">Link</a>
2024-09-04	[www.galgorm.com]	ransomhub	<a href="#">Link</a>
2024-09-04	[www.pcipa.com]	ransomhub	<a href="#">Link</a>
2024-09-04	[ych.com]	madliberator	<a href="#">Link</a>
2024-09-03	[idom.com]	lynx	<a href="#">Link</a>
2024-09-04	[plannedparenthood.org]	ransomhub	<a href="#">Link</a>
2024-09-04	[Sunrise Erectors]	hunters	<a href="#">Link</a>
2024-09-03	[simson-maxwell.com]	cactus	<a href="#">Link</a>
2024-09-03	[balboabayresort.com]	cactus	<a href="#">Link</a>
2024-09-03	[flodraulic.com]	cactus	<a href="#">Link</a>
2024-09-03	[mcphillips.co.uk]	cactus	<a href="#">Link</a>
2024-09-03	[rangeramerican.com]	cactus	<a href="#">Link</a>
2024-09-02	[Kingsport Imaging Systems]	medusa	<a href="#">Link</a>
2024-09-02	[Removal.AI]	ransomhub	<a href="#">Link</a>
2024-09-02	[Project Hospitality]	rhysida	<a href="#">Link</a>
2024-09-02	[Shomof Group]	medusa	<a href="#">Link</a>
2024-09-02	[www.sanyo-av.com]	ransomhub	<a href="#">Link</a>
2024-09-01	[Quálitas México]	hunters	<a href="#">Link</a>
2024-09-01	[welland]	trinity	<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.