

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240620



## 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>23</b>
5.0.1 Die nächste Wahnsinns-Möglichkeit für Angreifer, Software-Unternehmen zu hacken (VSCode Extensions) . . . . .	23
<b>6 Cyberangriffe: (Jun)</b>	<b>24</b>
<b>7 Ransomware-Erpressungen: (Jun)</b>	<b>25</b>
<b>8 Quellen</b>	<b>33</b>
8.1 Quellenverzeichnis . . . . .	33
<b>9 Impressum</b>	<b>34</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: Root-Lücke bedroht VMware vCenter Server***

Unter anderem zwei kritische Schwachstellen bedrohen vCenter Server und Cloud Foundation von VMware.

- [Link](#)

—

#### ***CISA warnt: Angriffe auf kritische Lücke in Progress Telerik Report Server***

In der Berichtsverwaltung Progress Telerik Report Server greifen Kriminelle eine Sicherheitslücke an. Sie erlaubt die Umgehung der Authentifizierung.

- [Link](#)

—

#### ***Nextcloud: Angreifer können Zwei-Faktor-Authentifizierung umgehen***

Die Clouddienst-Software Nextcloud ist verwundbar. In aktuellen Versionen haben die Entwickler mehrere Sicherheitslücken geschlossen.

- [Link](#)

—

#### ***Ivanti Endpoint Manager: Exploit für kritische Lücke aufgetaucht***

Ein Proof-of-Concept-Exploit für eine kritische Lücke in Ivanti Endpoint Manager ist aufgetaucht. Zudem gibt es ein Update für den Hotfix.

- [Link](#)

—

#### ***Sicherheitsupdates: Angreifer können Asus-Router kompromittieren***

Mehrere WLAN-Router von Asus sind verwundbar und Angreifer können auf sie zugreifen. Updates lösen mehrere Sicherheitsprobleme.

- [Link](#)

—

#### ***BIOS-Lücken: Angreifer können Dell-PCs kompromittieren***

Unter anderem PCs der Serie Alienware und Inspiron sind vor Attacks gefährdet. Dabei kann Schadcode auf Computer gelangen.

- [Link](#)

—

#### ***CISA warnt: Kritischer PHP-Bug wird von Ransomware ausgenutzt***

Automatisierte Attacks gegen Windows-Systeme mit PHP-CGI führen zur Infektion. Die Angreifer laden Schadcode nach und verschlüsseln den Server.

- [Link](#)

---

***Sicherheitsupdates: Fortinet rüstet Produkte gegen verschiedene Attacken***

Angreifer können Fortinet-Produkte unter anderem mit Schadcode attackieren, um Systeme zu kompromittieren. Patches stehen zum Download.

- [Link](#)

---

***Angreifer attackieren Geräte: Extra-Sicherheitsupdates für Google Pixel***

Patches schließen mehrere kritische Sicherheitslücken in Googles Pixel-Serie. Eine Schwachstelle soll bereits ausgenutzt werden.

- [Link](#)

---

***Sicherheitsupdate: VLC media player für Attacken anfällig***

Die Entwickler haben eine Sicherheitslücke im VLC media player geschlossen. Durch die Schwachstelle kann Schadcode schlüpfen.

- [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	0.958120000	0.994530000	<a href="#">Link</a>
CVE-2023-6553	0.918870000	0.989370000	<a href="#">Link</a>
CVE-2023-5360	0.911260000	0.988770000	<a href="#">Link</a>
CVE-2023-4966	0.969240000	0.997250000	<a href="#">Link</a>
CVE-2023-48795	0.961680000	0.995210000	<a href="#">Link</a>
CVE-2023-47246	0.943030000	0.991970000	<a href="#">Link</a>
CVE-2023-46805	0.955460000	0.994070000	<a href="#">Link</a>
CVE-2023-46747	0.972480000	0.998490000	<a href="#">Link</a>
CVE-2023-46604	0.931360000	0.990690000	<a href="#">Link</a>
CVE-2023-4542	0.924200000	0.989910000	<a href="#">Link</a>
CVE-2023-43208	0.959780000	0.994830000	<a href="#">Link</a>
CVE-2023-43177	0.960230000	0.994910000	<a href="#">Link</a>
CVE-2023-42793	0.970430000	0.997630000	<a href="#">Link</a>
CVE-2023-41265	0.920320000	0.989470000	<a href="#">Link</a>
CVE-2023-39143	0.948440000	0.992890000	<a href="#">Link</a>
CVE-2023-38646	0.900980000	0.988040000	<a href="#">Link</a>
CVE-2023-38205	0.945440000	0.992400000	<a href="#">Link</a>
CVE-2023-38203	0.968820000	0.997140000	<a href="#">Link</a>
CVE-2023-38146	0.905210000	0.988330000	<a href="#">Link</a>
CVE-2023-38035	0.974870000	0.999740000	<a href="#">Link</a>
CVE-2023-36845	0.966580000	0.996450000	<a href="#">Link</a>
CVE-2023-3519	0.912170000	0.988840000	<a href="#">Link</a>
CVE-2023-35082	0.967870000	0.996890000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.967810000	0.996860000	<a href="#">Link</a>
CVE-2023-34993	0.971450000	0.998060000	<a href="#">Link</a>
CVE-2023-34960	0.922740000	0.989680000	<a href="#">Link</a>
CVE-2023-34634	0.923550000	0.989770000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988430000	<a href="#">Link</a>
CVE-2023-34362	0.957100000	0.994360000	<a href="#">Link</a>
CVE-2023-34039	0.944630000	0.992260000	<a href="#">Link</a>
CVE-2023-3368	0.931130000	0.990650000	<a href="#">Link</a>
CVE-2023-33246	0.972320000	0.998450000	<a href="#">Link</a>
CVE-2023-32315	0.973460000	0.998960000	<a href="#">Link</a>
CVE-2023-30625	0.950680000	0.993250000	<a href="#">Link</a>
CVE-2023-30013	0.962250000	0.995300000	<a href="#">Link</a>
CVE-2023-29300	0.969840000	0.997440000	<a href="#">Link</a>
CVE-2023-29298	0.943950000	0.992120000	<a href="#">Link</a>
CVE-2023-28771	0.918640000	0.989350000	<a href="#">Link</a>
CVE-2023-28121	0.932700000	0.990840000	<a href="#">Link</a>
CVE-2023-27524	0.970620000	0.997700000	<a href="#">Link</a>
CVE-2023-27372	0.973630000	0.999040000	<a href="#">Link</a>
CVE-2023-27350	0.971140000	0.997930000	<a href="#">Link</a>
CVE-2023-26469	0.932230000	0.990800000	<a href="#">Link</a>
CVE-2023-26360	0.952190000	0.993500000	<a href="#">Link</a>
CVE-2023-26035	0.965720000	0.996230000	<a href="#">Link</a>
CVE-2023-25717	0.956860000	0.994310000	<a href="#">Link</a>
CVE-2023-25194	0.967930000	0.996920000	<a href="#">Link</a>
CVE-2023-2479	0.963760000	0.995700000	<a href="#">Link</a>
CVE-2023-24489	0.973550000	0.999000000	<a href="#">Link</a>
CVE-2023-23752	0.948880000	0.992980000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23397	0.915470000	0.989100000	<a href="#">Link</a>
CVE-2023-23333	0.963260000	0.995580000	<a href="#">Link</a>
CVE-2023-22527	0.972960000	0.998670000	<a href="#">Link</a>
CVE-2023-22518	0.965950000	0.996280000	<a href="#">Link</a>
CVE-2023-22515	0.973330000	0.998880000	<a href="#">Link</a>
CVE-2023-21839	0.955020000	0.993980000	<a href="#">Link</a>
CVE-2023-21554	0.955760000	0.994110000	<a href="#">Link</a>
CVE-2023-20887	0.966680000	0.996480000	<a href="#">Link</a>
CVE-2023-1671	0.964510000	0.995860000	<a href="#">Link</a>
CVE-2023-0669	0.968870000	0.997150000	<a href="#">Link</a>

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

Wed, 19 Jun 2024

#### **[UPDATE] [hoch] GNU libc: mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um beliebigen Programmcode mit den Rechten des Angegriffenen auszuführen oder einen Denial of Service Angriff durchführen.

- [Link](#)

—

Wed, 19 Jun 2024

#### **[UPDATE] [kritisch] GNU libc: Mehrere Schwachstellen ermöglichen Codeausführung und Denial of Service**

Ein Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Wed, 19 Jun 2024

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

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu



verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 19 Jun 2024

**[NEU] [hoch] Google Chrome: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen, Sicherheitsmechanismen zu umgehen und möglicherweise andere nicht spezifizierte Auswirkungen zu haben.

- [Link](#)

—

Wed, 19 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Code auszuführen, um einen Denial of Service Zustand herbeizuführen und um Sicherheitsmechanismen zu umgehen, sowie den Benutzer zu täuschen.

- [Link](#)

—

Wed, 19 Jun 2024

**[UPDATE] [hoch] Red Hat Advanced Cluster Management for Kubernetes: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Red Hat Advanced Cluster Management for Kubernetes ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 19 Jun 2024

**[UPDATE] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Dateien zu manipulieren oder Informationen offenzulegen.

- [Link](#)

—

Wed, 19 Jun 2024

**[UPDATE] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Daten**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Daten zu manipulieren oder Informationen offenzulegen.

- [Link](#)

—

Wed, 19 Jun 2024

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

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 19 Jun 2024

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

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreifer kann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und die Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Wed, 19 Jun 2024

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

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

- [Link](#)

—

Wed, 19 Jun 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Dateien zu manipulieren, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder um weitere nicht spezifizierte Angriffe auszuführen.

- [Link](#)

—

Wed, 19 Jun 2024

**[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- [Link](#)

—

Wed, 19 Jun 2024

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

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

- [Link](#)

—  
Wed, 19 Jun 2024

**[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—  
Wed, 19 Jun 2024

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

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

- [Link](#)

—  
Wed, 19 Jun 2024

**[UPDATE] [hoch] Red Hat OpenShift Service Mesh Containers: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Service Mesh Containers ausnutzen, um Dateien zu manipulieren, einen 'Denial of Service'-Zustand erzeugen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder weitere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—  
Tue, 18 Jun 2024

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

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

- [Link](#)

—  
Tue, 18 Jun 2024

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

Ein entfernter anonym Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—  
Tue, 18 Jun 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
6/19/2024	[Ubuntu 20.04 LTS : Git vulnerability (USN-6793-2)]	critical
6/18/2024	[Google Chrome < 126.0.6478.114 Multiple Vulnerabilities]	critical
6/18/2024	[Google Chrome < 126.0.6478.114 Multiple Vulnerabilities]	critical
6/18/2024	[Sensormatic Electronics Illustra Pro Gen 4 Active Debug Code (CVE-2023-0954)]	critical
6/19/2024	[Ubuntu 22.04 LTS : Linux kernel (HWE) vulnerabilities (USN-6818-4)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-1_1 (SUSE-SU-2024:2059-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libaom (SUSE-SU-2024:2056-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-3 (SUSE-SU-2024:2066-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-Authlib (SUSE-SU-2024:2064-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xdg-desktop-portal (SUSE-SU-2024:2067-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:2073-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-1_1 (SUSE-SU-2024:2051-1)]	high

Datum	Schwachstelle	Bewertung
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaFirefox (SUSE-SU-2024:2061-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : less (SUSE-SU-2024:2060-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : webkit2gtk3 (SUSE-SU-2024:2065-1)]	high
6/19/2024	[openSUSE 15 Security Update : gdcmm (openSUSE-SU-2024:0167-1)]	high
6/19/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thunderbird vulnerabilities (USN-6840-1)]	high
6/19/2024	[CentOS 7 : ipa (RHSA-2024:3760)]	high
6/19/2024	[CentOS 7 : firefox (RHSA-2024:3951)]	high
6/19/2024	[CentOS 7 : bind, bind-dyndb-ldap, and dhcp (RHSA-2024:3741)]	high
6/19/2024	[SUSE SLES15 Security Update : podman (SUSE-SU-2024:2050-1)]	high
6/19/2024	[SUSE SLED15 / SLES15 Security Update : python-Werkzeug (SUSE-SU-2024:1591-2)]	high
6/19/2024	[AlmaLinux 8 : flatpak (ALSA-2024:3961)]	high
6/19/2024	[FreeBSD : chromium – multiple security fixes (453aa0fc-2d91-11ef-8a0f-a8a1599412c6)]	high
6/19/2024	[AlmaLinux 9 : firefox (ALSA-2024:3955)]	high
6/19/2024	[AlmaLinux 9 : flatpak (ALSA-2024:3959)]	high
6/19/2024	[AlmaLinux 8 : firefox (ALSA-2024:3954)]	high
6/19/2024	[Oracle Linux 7 : glibc (ELSA-2024-12444)]	high
6/19/2024	[Debian dla-3836 : thunderbird - security update]	high
6/18/2024	[RHEL 8 : flatpak (RHSA-2024:3979)]	high
6/18/2024	[RHEL 7 : flatpak (RHSA-2024:3980)]	high
6/18/2024	[Oracle Linux 7 : flatpak (ELSA-2024-3980)]	high

Datum	Schwachstelle	Bewertung
6/18/2024	[Oracle Linux 7 : glibc (ELSA-2024-12442)]	high
6/18/2024	[Fedora 40 : webkitgtk (2024-4d71f28349)]	high
6/18/2024	[Debian dsa-5715 : composer - security update]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Wed, 19 Jun 2024

#### ***Bagisto 2.1.2 Client-Side Template Injection***

Bagisto version 2.1.2 suffers from a client-side template injection vulnerability.

- [Link](#)

—

” “Wed, 19 Jun 2024

#### ***User Registration And Management System 3.2 SQL Injection***

User Registration and Management System version 3.2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Tue, 18 Jun 2024

#### ***PHP CGI Argument Injection Remote Code Execution***

This Metasploit module exploits a PHP CGI argument injection vulnerability affecting PHP in certain configurations on a Windows target. A vulnerable configuration is locale dependant (such as Chinese or Japanese), such that the Unicode best-fit conversion scheme will unexpectedly convert a soft hyphen (0xAD) into a dash (0x2D) character. Additionally a target web server must be configured to run PHP under CGI mode, or directly expose the PHP binary. This issue has been fixed in PHP 8.3.8 (for the 8.3.x branch), 8.2.20 (for the 8.2.x branch), and 8.1.29 (for the 8.1.x branch). PHP 8.0.x and below are end of life and have not received patches. XAMPP is vulnerable in a default configuration, and we can target the /php-cgi/php-cgi.exe endpoint. To target an explicit .php endpoint (e.g. /index.php), the server must be configured to run PHP scripts in CGI mode.

- [Link](#)

—

” “Tue, 18 Jun 2024

#### ***Apache OFBiz Forgot Password Directory Traversal***

Apache OFBiz versions prior to 18.12.13 are vulnerable to a path traversal vulnerability. The vulnerable endpoint /webtools/control/forgotPassword allows an attacker to access the ProgramExport endpoint which in turn allows for remote code execution in the context of the user running the application.

- [Link](#)

---

” “Tue, 18 Jun 2024

***PowerVR Out-Of-Bounds Write***

PowerVR suffers from an out-of-bounds write of firmware addresses in PVRSRVRGXXKickTA3DKM().

- [Link](#)

---

” “Tue, 18 Jun 2024

***PowerVR Uninitialized Memory Disclosure***

PowerVR suffers from an uninitialized memory disclosure and crash due to out-of-bounds reads in hwperf\_host\_%d stream.

- [Link](#)

---

” “Tue, 18 Jun 2024

***Microweber 2.0.15 Cross Site Scripting***

Microweber version 2.0.15 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

---

” “Tue, 18 Jun 2024

***Backdoor.Win32.Plugx MVID-2024-0686 Insecure Permissions***

Backdoor.Win32.Plugx malware suffers from an insecure permissions vulnerability.

- [Link](#)

---

” “Mon, 17 Jun 2024

***SPA-CART CMS 1.9.0.6 Username Enumeration / Business Logic Flaw***

SPA-CART CMS version 1.9.0.6 suffers from business logic and user enumeration flaws.

- [Link](#)

---

” “Mon, 17 Jun 2024

***Payroll Management System 1.0 Remote Code Execution***

Payroll Management System version 1.0 suffers from a remote code execution vulnerability.

- [Link](#)

---

” “Mon, 17 Jun 2024

**WordPress RFC WordPress 6.0.8 Shell Upload**

WordPress RFC WordPress plugin version 6.0.8 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Fri, 14 Jun 2024

**Premium Support Tickets For WHMCS 1.2.10 Cross Site Scripting**

Premium Support Tickets For WHMCS version 1.2.10 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 14 Jun 2024

**AEGON LIFE 1.0 Cross Site Scripting**

AEGON LIFE version 1.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 14 Jun 2024

**AEGON LIFE 1.0 Remote Code Execution**

AEGON LIFE version 1.0 suffers from an unauthenticated remote code execution vulnerability.

- [Link](#)

—

” “Fri, 14 Jun 2024

**AEGON LIFE 1.0 SQL Injection**

AEGON LIFE version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Fri, 14 Jun 2024

**PHP Remote Code Execution**

PHP versions prior to 8.3.8 suffer from a remote code execution vulnerability.

- [Link](#)

—

” “Thu, 13 Jun 2024

**Telerik Report Server Authentication Bypass / Remote Code Execution**

This Metasploit module chains an authentication bypass vulnerability with a deserialization vulnerability to obtain remote code execution against Telerik Report Server versions 10.0.24.130 and below. The authentication bypass flaw allows an unauthenticated user to create a new user with administrative privileges. The USERNAME datastore option can be used to authenticate with an existing account to prevent the creation of a new one. The deserialization flaw works by uploading a specially crafted report that when loaded will execute an OS command as NT AUTHORITY\SYSTEM. The module will automatically delete the created report but not the account because users are



unable to delete themselves.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Rejetto HTTP File Server (HFS) Unauthenticated Remote Code Execution***

The Rejetto HTTP File Server (HFS) version 2.x is vulnerable to an unauthenticated server side template injection (SSTI) vulnerability. A remote unauthenticated attacker can execute code with the privileges of the user account running the HFS.exe server process. This exploit has been tested to work against version 2.4.0 RC7 and 2.3m. The Rejetto HTTP File Server (HFS) version 2.x is no longer supported by the maintainers and no patch is available. Users are recommended to upgrade to newer supported versions.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Cacti Import Packages Remote Code Execution***

This exploit module leverages an arbitrary file write vulnerability in Cacti versions prior to 1.2.27 to achieve remote code execution. It abuses the Import Packages feature to upload a specially crafted package that embeds a PHP file. Cacti will extract this file to an accessible location. The module finally triggers the payload to execute arbitrary PHP code in the context of the user running the web server. Authentication is needed and the account must have access to the Import Packages feature. This is granted by setting the Import Templates permission in the Template Editor section.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Lost And Found Information System 1.0 Cross Site Scripting***

Lost and Found Information System version 1.0 suffers from a reflective cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Lost And Found Information System 1.0 SQL Injection***

Lost and Found Information System version 1.0 suffers from an unauthenticated blind boolean-based remote SQL injection vulnerability.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Lost And Found Information System 1.0 SQL Injection***

Lost and Found Information System version 1.0 suffers from an unauthenticated blind time-based

remote SQL injection vulnerability.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Lost And Found Information System 1.0 Cross Site Scripting***

Lost and Found Information System version 1.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Quick Cart 6.7 Shell Upload***

Quick Cart version 6.7 suffers from a remote shell upload vulnerability provided you have administrative privileges.

- [Link](#)

—

” “Thu, 13 Jun 2024

***Quick CMS 6.7 Shell Upload***

Quick CMS version 6.7 suffers from a remote shell upload vulnerability provided you have administrative privileges.

- [Link](#)

—

”

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

“Tue, 18 Jun 2024

***ZDI-24-815: Toshiba e-STUDIO2518A vsftpd Incorrect Permission Assignment Privilege Escalation Vulnerability***

- [Link](#)

—

” “Tue, 18 Jun 2024

***ZDI-24-814: Toshiba e-STUDIO2518A unzip Directory Traversal Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 18 Jun 2024

***ZDI-24-813: Toshiba e-STUDIO2518A Authentication Bypass Vulnerability***

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-812: Hewlett Packard Enterprise OneView Apache Server-Side Request Forgery Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-811: Hewlett Packard Enterprise OneView clusterService Authentication Bypass Denial-of-Service Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-810: Hewlett Packard Enterprise OneView startUpgradeCommon Command Injection Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-809: (0Day) Actiontec WCB6200Q uh\_get\_postdata\_withupload Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-808: (0Day) Actiontec WCB6200Q Cookie Format String Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-807: (0Day) Actiontec WCB6200Q Multipart Boundary Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-806: (0Day) Actiontec WCB6200Q uh\_tcp\_recv\_header Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-805: (0Day) Actiontec WCB6200Q uh\_tcp\_recv\_content Buffer Overflow Remote Code Exe-**

**cution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-804: Parallels Desktop Toolgate Heap-based Buffer Overflow Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-803: Parallels Desktop Updater Protection Mechanism Failure Software Downgrade Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-802: (0Day) Poly Plantronics Hub Link Following Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-801: Tenable Nessus Network Monitor Uncontrolled Search Path Element Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-800: (0Day) Autodesk AutoCAD SLDASM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-799: (0Day) Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-798: (0Day) Autodesk AutoCAD IGES File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-797: (0Day) Autodesk AutoCAD 3DM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-796: (0Day) Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-795: (0Day) Autodesk AutoCAD MODEL File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-794: (0Day) Autodesk AutoCAD STP File Parsing Uninitialized Variable Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-793: (0Day) Autodesk AutoCAD 3DM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-792: (0Day) Autodesk AutoCAD PRT File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-791: (0Day) Autodesk AutoCAD 3DM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-790: (0Day) Autodesk AutoCAD SLDPRT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-789: (0Day) Autodesk AutoCAD 3DM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-788: (0Day) Autodesk AutoCAD 3DM File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-787: (0Day) Autodesk AutoCAD MODEL File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-786: PaperCut NG print.script.sandboxed Exposed Dangerous Function Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-785: PaperCut MF EmailRenderer Server-Side Template Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-784: PaperCut MF handleServiceException Cross-Site Scripting Authentication Bypass Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-783: PaperCut MF pc-upconnector-service Server-Side Request Forgery Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 18 Jun 2024

**ZDI-24-782: PaperCut NG PrintDeployProxyController Incorrect Authorization Authentication By-**

***pass Vulnerability***

- [Link](#)

—

” “Tue, 18 Jun 2024

***ZDI-24-781: PaperCut NG generateNextFileName Directory Traversal Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 18 Jun 2024

***ZDI-24-780: PaperCut NG upload Link Following Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 18 Jun 2024

***ZDI-24-779: PaperCut NG VendorKeys Hardcoded Credentials Authentication Bypass Vulnerability***

- [Link](#)

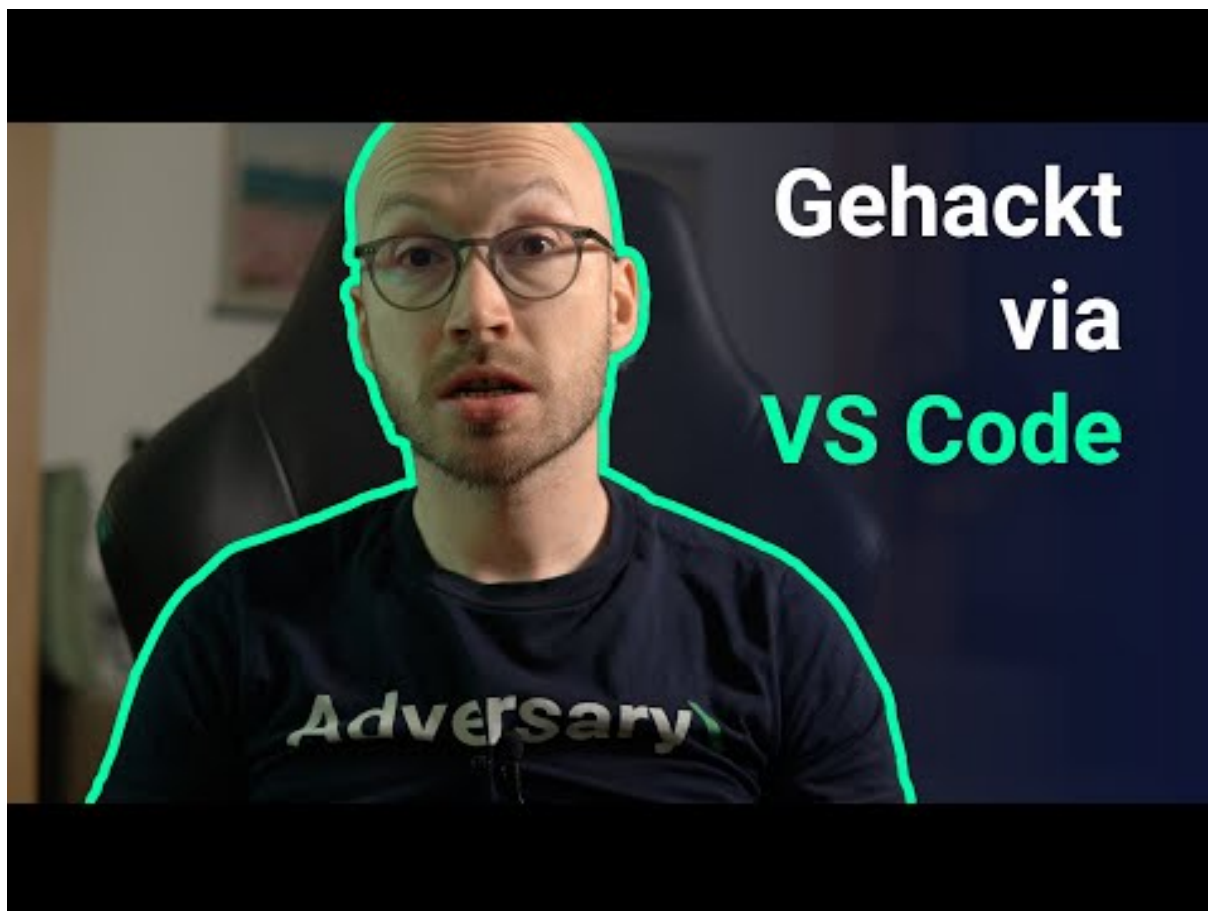
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Die nächste Wahnsinns-Möglichkeit für Angreifer, Software-Unternehmen zu hacken (VSCode Extensions)



[Zum Youtube Video](#)



## 6 Cyberangriffe: (Jun)

Datum	Opfer	Land	Information
2024-06-19	CDK	[USA]	<a href="#">Link</a>
2024-06-17	MARINA (Maritime Industry Authority)	[PHL]	<a href="#">Link</a>
2024-06-17	Rekah	[ISR]	<a href="#">Link</a>
2024-06-17	Krankenhaus Agatharied	[DEU]	<a href="#">Link</a>
2024-06-16	Oahu Transit Services (OTS)	[USA]	<a href="#">Link</a>
2024-06-16	ØØØ (Junsi Group) et Brooks Brothers	[HKG]	<a href="#">Link</a>
2024-06-14	GlobalWafers	[TWN]	<a href="#">Link</a>
2024-06-13	Globe Life Inc.	[USA]	<a href="#">Link</a>
2024-06-12	Axido	[FRA]	<a href="#">Link</a>
2024-06-12	Commune de Benalmádena	[ESP]	<a href="#">Link</a>
2024-06-12	Richland School District	[USA]	<a href="#">Link</a>
2024-06-11	Mercatino dell'usato	[ITA]	<a href="#">Link</a>
2024-06-10	Toronto District School Board (TDSB)	[CAN]	<a href="#">Link</a>
2024-06-10	Crown Equipment Corporation	[USA]	<a href="#">Link</a>
2024-06-09	Cleveland	[USA]	<a href="#">Link</a>
2024-06-09	Hands, The Family Network	[CAN]	<a href="#">Link</a>
2024-06-09	Emcali	[COL]	<a href="#">Link</a>
2024-06-08	KADOKAWA	[JPN]	<a href="#">Link</a>
2024-06-08	Mobile County Health Department	[USA]	<a href="#">Link</a>
2024-06-08	Findlay Automotive Group	[USA]	<a href="#">Link</a>
2024-06-06	ASST Rhodense	[ITA]	<a href="#">Link</a>
2024-06-04	Vietnam Post Corporation (Vietnam Post)	[VNM]	<a href="#">Link</a>
2024-06-04	Synnovis	[GBR]	<a href="#">Link</a>
2024-06-04	Groupe IPM	[BEL]	<a href="#">Link</a>
2024-06-02	Institut technologique de Sonora (Itson)	[MEX]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-06-02	Special Health Resources (SHR)	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Jun)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-04	[SAWA INTERNATIONAL]	spacebears	<a href="#">Link</a>
2024-06-18	[Ojai srl]	8base	<a href="#">Link</a>
2024-06-19	[<www.invisio.com>]	ransomhub	<a href="#">Link</a>
2024-06-19	[Behavioral Health Response (bhr.local)]	incransom	<a href="#">Link</a>
2024-06-19	[Synnovis]	qilin	<a href="#">Link</a>
2024-06-19	[suminoe.us]	cactus	<a href="#">Link</a>
2024-06-19	[Lindermayr]	akira	<a href="#">Link</a>
2024-06-19	[Perfumes & Companhia]	akira	<a href="#">Link</a>
2024-06-19	[First Baptist Medical Center]	moneymessage	<a href="#">Link</a>
2024-06-11	[DERBY SCHOOL]	incransom	<a href="#">Link</a>
2024-06-18	[Circle K Atlanta]	hunters	<a href="#">Link</a>
2024-06-16	[kinslerfamilydentistry]	qilin	<a href="#">Link</a>
2024-06-18	[sofidel.com]	cactus	<a href="#">Link</a>
2024-06-18	[sky-light.com]	cactus	<a href="#">Link</a>
2024-06-18	[reawire.com]	cactus	<a href="#">Link</a>
2024-06-18	[malca-amit.com]	abyss	<a href="#">Link</a>
2024-06-17	[www.gbricambi.it]	ransomhub	<a href="#">Link</a>
2024-06-10	[OCEANAIR]	incransom	<a href="#">Link</a>
2024-06-17	[The Kansas City Kansas Police Department]	blacksuit	<a href="#">Link</a>
2024-06-04	[northcottage.com]	qilin	<a href="#">Link</a>
2024-06-17	[A-Line Staffing Solutions]	underground	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-13	[www.racalacoustics.com [UPDATE]]	ransomhub	Link
2024-06-17	[www.liderit.es]	ransomhub	Link
2024-06-17	[St Vincent de Paul Catholic School]	qilin	Link
2024-06-17	[Sensory Spectrum]	incransom	Link
2024-06-17	[Acteon Group]	hunters	Link
2024-06-17	[pkaufmann.com]	blackbasta	Link
2024-06-17	[modplan.co.uk]	blackbasta	Link
2024-06-17	[wielton.com.pl]	blackbasta	Link
2024-06-17	[grupoamper.com]	blackbasta	Link
2024-06-17	[TETRA Technologies, Inc.]	akira	Link
2024-06-16	[parlorenzo.com]	ransomhub	Link
2024-06-17	[www.domainatcleveland.com]	ransomhub	Link
2024-06-01	[Virum Apotek]	ransomhouse	Link
2024-06-17	[SolidCAM 2024 SP0]	handala	Link
2024-06-17	[Next Step Healthcare]	qilin	Link
2024-06-17	[cosimti.com]	darkvault	Link
2024-06-17	[fifcousa.com]	dAn0n	Link
2024-06-17	[mgfsourcing.com]	blackbasta	Link
2024-06-17	[journohq.com]	darkvault	Link
2024-06-16	[colfax.k12.wi.us]	blacksuit	Link
2024-06-16	[Production Machine & Enterprises]	rhysida	Link
2024-06-16	[CETOS Services]	rhysida	Link
2024-06-15	[Kiemle-Hankins]	rhysida	Link
2024-06-15	[Legrand CRM]	hunters	Link
2024-06-15	[MRI]	hunters	Link
2024-06-15	[Ma'agan Michael Kibbutz]	handala	Link
2024-06-15	[Oahu Transit Services]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-12	[Sun City Pediatrics PA (USA, TX)]	spacebears	<a href="#">Link</a>
2024-06-11	[Lee Trevino Dental (USA,TX)]	spacebears	<a href="#">Link</a>
2024-06-15	[Peregrine Petroleum]	blacksuit	<a href="#">Link</a>
2024-06-15	[Mountjoy]	bianlian	<a href="#">Link</a>
2024-06-14	[svmasonry.com]	qilin	<a href="#">Link</a>
2024-06-14	[MBE CPA]	metaencryptor	<a href="#">Link</a>
2024-06-14	[EnviroApplications]	qilin	<a href="#">Link</a>
2024-06-14	[www.gannons.co.uk]	apt73	<a href="#">Link</a>
2024-06-14	[New Balance Commodities]	akira	<a href="#">Link</a>
2024-06-14	[Victoria Racing Club]	medusa	<a href="#">Link</a>
2024-06-14	[Mundocar.eu]	cloak	<a href="#">Link</a>
2024-06-13	[Cukierski & Associates, LLC]	everest	<a href="#">Link</a>
2024-06-13	[Diogenet S.r.l.]	everest	<a href="#">Link</a>
2024-06-13	[2K Dental]	everest	<a href="#">Link</a>
2024-06-13	[Dordt University]	bianlian	<a href="#">Link</a>
2024-06-13	[Borrer Executive Search]	apt73	<a href="#">Link</a>
2024-06-13	[www.bigalsfoodservice.co.uk]	apt73	<a href="#">Link</a>
2024-06-13	[www.racalacoustics.com]	ransomhub	<a href="#">Link</a>
2024-06-13	[Kito Canada]	incransom	<a href="#">Link</a>
2024-06-11	[Bock & Associates, LLP]	qilin	<a href="#">Link</a>
2024-06-12	[Walder Wyss and Partners]	play	<a href="#">Link</a>
2024-06-12	[Celluphone]	play	<a href="#">Link</a>
2024-06-12	[Me Too Shoes]	play	<a href="#">Link</a>
2024-06-12	[Ab Monstera Metall]	play	<a href="#">Link</a>
2024-06-12	[Amarilla Gas]	play	<a href="#">Link</a>
2024-06-12	[Aldenhoven]	play	<a href="#">Link</a>
2024-06-12	[ANTECH-GUTLING Gruppe]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-12	[Refcio & Associates]	play	<a href="#">Link</a>
2024-06-12	[City Builders]	play	<a href="#">Link</a>
2024-06-12	[Eurotrol B.V.]	blacksuit	<a href="#">Link</a>
2024-06-12	[Seagulf Marine Industries]	play	<a href="#">Link</a>
2024-06-12	[Western Mechanical]	play	<a href="#">Link</a>
2024-06-12	[Trisun Land Services]	play	<a href="#">Link</a>
2024-06-10	[GEMCO Constructors ]	medusa	<a href="#">Link</a>
2024-06-10	[Dynamo Electric ]	medusa	<a href="#">Link</a>
2024-06-11	[Farnell Packaging]	medusa	<a href="#">Link</a>
2024-06-12	[hydefuel.com]	qilin	<a href="#">Link</a>
2024-06-12	[Diverse Technology Industrial]	play	<a href="#">Link</a>
2024-06-12	[Air Cleaning Specialists]	play	<a href="#">Link</a>
2024-06-12	[Corbin Turf & Ornamental Supply]	play	<a href="#">Link</a>
2024-06-12	[Kinter]	play	<a href="#">Link</a>
2024-06-12	[Goodman Reichwald-Dodge]	play	<a href="#">Link</a>
2024-06-12	[3GL Technology Solutions]	play	<a href="#">Link</a>
2024-06-12	[Brainworks Software]	play	<a href="#">Link</a>
2024-06-12	[Eagle Materials]	play	<a href="#">Link</a>
2024-06-12	[Great Lakes International Trading]	play	<a href="#">Link</a>
2024-06-12	[Smartweb]	play	<a href="#">Link</a>
2024-06-12	[Peterbilt of Atlanta]	play	<a href="#">Link</a>
2024-06-12	[Chroma Color]	play	<a href="#">Link</a>
2024-06-12	[Shinnick & Ryan]	play	<a href="#">Link</a>
2024-06-12	[ZeepLive]	darkvault	<a href="#">Link</a>
2024-06-12	[Concrete]	hunters	<a href="#">Link</a>
2024-06-12	[IPM Group (Multimedia Information & Production Company)]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-12	[manncorp.com]	lockbit3	<a href="#">Link</a>
2024-06-12	[sgvfr.com]	trinity	<a href="#">Link</a>
2024-06-12	[CBSTRAINING]	trinity	<a href="#">Link</a>
2024-06-11	[Kutes.com]	redransomware	<a href="#">Link</a>
2024-06-11	[www.novabitsrl.it]	ransomhub	<a href="#">Link</a>
2024-06-11	[smicusa.com]	ransomhub	<a href="#">Link</a>
2024-06-11	[www.ham.org.br]	ransomhub	<a href="#">Link</a>
2024-06-12	[NJORALSURGERY.COM]	clop	<a href="#">Link</a>
2024-06-11	[SolidCAM LEAK]	handala	<a href="#">Link</a>
2024-06-12	[Zuber Gardner CPAs pt.2]	everest	<a href="#">Link</a>
2024-06-09	[Seafrigo]	dragonforce	<a href="#">Link</a>
2024-06-12	[Special Health Resources]	blacksuit	<a href="#">Link</a>
2024-06-11	[WinFashion ERP]	arcusmedia	<a href="#">Link</a>
2024-06-12	[apex.uk.net]	apt73	<a href="#">Link</a>
2024-06-12	[AlphaNovaCapital]	apt73	<a href="#">Link</a>
2024-06-12	[AMI Global Assistance]	apt73	<a href="#">Link</a>
2024-06-06	[filmetrics corporation]	trinity	<a href="#">Link</a>
2024-06-11	[Embotits Espina, SLU]	8base	<a href="#">Link</a>
2024-06-10	[a-agroup]	qilin	<a href="#">Link</a>
2024-06-10	[Harper Industries]	hunters	<a href="#">Link</a>
2024-06-10	[nordspace.lt]	darkvault	<a href="#">Link</a>
2024-06-05	[www.ugrocapital.com]	ransomhub	<a href="#">Link</a>
2024-06-10	[Arge Baustahl]	akira	<a href="#">Link</a>
2024-06-10	[transportlaberge.com]	cactus	<a href="#">Link</a>
2024-06-10	[sanyo-shokai.co.jp]	cactus	<a href="#">Link</a>
2024-06-10	[wave2.co.kr]	darkvault	<a href="#">Link</a>
2024-06-10	[jmthompson.com]	cactus	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-10	[ctsystem.com]	cactus	<a href="#">Link</a>
2024-06-10	[ctgbrands.com]	cactus	<a href="#">Link</a>
2024-06-10	[SolidCAM]	handala	<a href="#">Link</a>
2024-06-08	[EvoEvents]	dragonforce	<a href="#">Link</a>
2024-06-08	[Barrett Eye Care]	dragonforce	<a href="#">Link</a>
2024-06-08	[Parrish-McCall Constructors]	dragonforce	<a href="#">Link</a>
2024-06-08	[California Rice Exchange]	rhysida	<a href="#">Link</a>
2024-06-07	[Allied Toyota Lift]	qilin	<a href="#">Link</a>
2024-06-08	[Hoppecke]	dragonforce	<a href="#">Link</a>
2024-06-07	[Elite Limousine Plus Inc]	bianlian	<a href="#">Link</a>
2024-06-07	[ccmaui.org]	lockbit3	<a href="#">Link</a>
2024-06-07	[talalayglobal.com]	blackbasta	<a href="#">Link</a>
2024-06-07	[akdenizchemson.com]	blackbasta	<a href="#">Link</a>
2024-06-07	[Reinhold Sign Service]	akira	<a href="#">Link</a>
2024-06-07	[Axi Energy Services]	hunters	<a href="#">Link</a>
2024-06-06	[RAVEN Mechanical]	hunters	<a href="#">Link</a>
2024-06-06	[dmedelivers.com]	embargo	<a href="#">Link</a>
2024-06-06	[fpr-us.com]	cactus	<a href="#">Link</a>
2024-06-06	[TBMCG.com]	ElDorado	<a href="#">Link</a>
2024-06-06	[www.vet.k-state.edu]	ElDorado	<a href="#">Link</a>
2024-06-06	[www.uccretrievals.com]	ElDorado	<a href="#">Link</a>
2024-06-06	[robson.com]	blackbasta	<a href="#">Link</a>
2024-06-06	[elutia.com]	blackbasta	<a href="#">Link</a>
2024-06-06	[ssiworld.com]	blackbasta	<a href="#">Link</a>
2024-06-06	[driver-group.com]	blackbasta	<a href="#">Link</a>
2024-06-06	[HTE Technologies]	ElDorado	<a href="#">Link</a>
2024-06-06	[goughhomes.com]	ElDorado	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-06	[Baker Triangle]	ElDorado	<a href="#">Link</a>
2024-06-06	[www.tankerska.hr]	ElDorado	<a href="#">Link</a>
2024-06-06	[cityofpensacola.com]	ElDorado	<a href="#">Link</a>
2024-06-06	[thunderbirdcc.org]	ElDorado	<a href="#">Link</a>
2024-06-06	[www.itasnatta.edu.it]	ElDorado	<a href="#">Link</a>
2024-06-06	[panzersolutions.com]	ElDorado	<a href="#">Link</a>
2024-06-06	[lindostar.it]	ElDorado	<a href="#">Link</a>
2024-06-06	[burotec.biz]	ElDorado	<a href="#">Link</a>
2024-06-06	[celplan.com]	ElDorado	<a href="#">Link</a>
2024-06-06	[adamshomes.com]	ElDorado	<a href="#">Link</a>
2024-06-06	[dynasafe.com]	blackbasta	<a href="#">Link</a>
2024-06-06	[Panasonic Australia]	akira	<a href="#">Link</a>
2024-06-04	[Health People]	medusa	<a href="#">Link</a>
2024-06-04	[IPPBX ]	medusa	<a href="#">Link</a>
2024-06-04	[Market Pioneer International Corp]	medusa	<a href="#">Link</a>
2024-06-04	[Mercy Drive Inc]	medusa	<a href="#">Link</a>
2024-06-04	[Radiosurgery New York ]	medusa	<a href="#">Link</a>
2024-06-04	[Inside Broadway]	medusa	<a href="#">Link</a>
2024-06-04	[Oracle Advisory Services ]	medusa	<a href="#">Link</a>
2024-06-04	[Women's Sports Foundation]	medusa	<a href="#">Link</a>
2024-06-05	[“Moshe Kahn Advocates”]	mallox	<a href="#">Link</a>
2024-06-05	[craigsteven.com]	lockbit3	<a href="#">Link</a>
2024-06-05	[Elfi-Tech]	handala	<a href="#">Link</a>
2024-06-05	[Dubai Municipality (UAE)]	daixin	<a href="#">Link</a>
2024-06-05	[E-T-A]	akira	<a href="#">Link</a>
2024-06-01	[Frontier.com]	ransomhub	<a href="#">Link</a>
2024-06-04	[Premium Broking House]	SenSayQ	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-06-04	[Vimer Industrie Grafiche Italiane]	SenSayQ	<a href="#">Link</a>
2024-06-04	[Voorhees Family Office Services]	everest	<a href="#">Link</a>
2024-06-04	[Mahindra Racing]	akira	<a href="#">Link</a>
2024-06-04	[naprodgroup.com]	lockbit3	<a href="#">Link</a>
2024-06-03	[Madata Data Collection & Internet Portals]	mallox	<a href="#">Link</a>
2024-06-03	[Río Negro]	mallox	<a href="#">Link</a>
2024-06-03	[Langescheid GbR]	arcusmedia	<a href="#">Link</a>
2024-06-03	[Franja IT Integradores de Tecnología]	arcusmedia	<a href="#">Link</a>
2024-06-03	[Duque Saldarriaga]	arcusmedia	<a href="#">Link</a>
2024-06-03	[BHMACH]	arcusmedia	<a href="#">Link</a>
2024-06-03	[Botselo]	arcusmedia	<a href="#">Link</a>
2024-06-03	[Immediate Transport – UK]	arcusmedia	<a href="#">Link</a>
2024-06-01	[cfymca.org]	lockbit3	<a href="#">Link</a>
2024-06-03	[Northern Minerals Limited]	bianlian	<a href="#">Link</a>
2024-06-03	[ISETO CORPORATION]	8base	<a href="#">Link</a>
2024-06-03	[Nidec Motor Corporation]	8base	<a href="#">Link</a>
2024-06-03	[Anderson Mikos Architects]	akira	<a href="#">Link</a>
2024-06-03	[My City application]	handala	<a href="#">Link</a>
2024-06-02	[www.eastshoresound.com]	ransomhub	<a href="#">Link</a>
2024-06-02	[smithandcaugheys.co.nz]	lockbit3	<a href="#">Link</a>
2024-06-01	[Frontier ]	ransomhub	<a href="#">Link</a>
2024-06-16	[garrettmotion.com]	dispossessor	<a href="#">Link</a>
2024-06-28	[notablefrontier.com]	dispossessor	<a href="#">Link</a>
2024-06-12	[energytransfer.com]	dispossessor	<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.