

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240416



## 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>18</b>
5.0.1 Oh wow, this was very close: xz-utils was backdoored ☒ . . . . .	18
<b>6 Cyberangriffe: (Apr)</b>	<b>19</b>
<b>7 Ransomware-Erpressungen: (Apr)</b>	<b>19</b>
<b>8 Quellen</b>	<b>28</b>
8.1 Quellenverzeichnis . . . . .	28
<b>9 Impressum</b>	<b>29</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

#### ***Lancom-Setup-Assistent leert Root-Passwort***

Wer Lancom-Router mit dem Windows-Setup-Assistenten konfiguriert, läuft Gefahr, das Root-Passwort durch ein leeres zu ersetzen.

- [Link](#)

—

#### ***Sicherheitsupdates: Schwachstellen in PHP gefährden Websites***

Die PHP-Entwickler haben mehrere Schwachstellen geschlossen. Eine Sicherheitslücke gilt als kritisch.

- [Link](#)

—

#### ***BSI warnt vor aktiv angegriffener Sicherheitslücke in Palo-Alto-Firewalls***

Das BSI warnt vor einer kritischen Sicherheitslücke in Firewalls von Palo Alto Networks. Sie wird bereits attackiert. Angreifer erhalten root-Zugriff.

- [Link](#)

—

#### ***Sicherheitslücken: Angreifer können Juniper-Netzwerkgeräte lahmlegen***

Wichtige Patches schließen mehrere Schwachstellen in Junos OS, die Firewalls, Router und Switches verwundbar machen.

- [Link](#)

—

#### ***WLAN-Access-Points von TP-Link 15 Minuten lang nach Reboot attackierbar***

Zwei TP-Link-WLAN-Access-Points sind unter anderem für DoS-Attacken anfällig. Sicherheitsupdates sind verfügbar.

- [Link](#)

—

#### ***Google Chrome: Sandbox-Ausbruch durch bestimmte Gesten möglich***

Google hat den Chrome-Webbrowser aktualisiert. Angreifer können Sicherheitslücken zum Ausführen von Schadcode missbrauchen.

- [Link](#)

—

#### ***Befehlsschmuggel: Kritische Lücke in Programmiersprachen unter Windows***

BatBadBut heißt eine kritische Befehlsschmuggel-Lücke, die mehrere Programmiersprachen unter Windows betrifft. Abhilfe ist schwer.

- [Link](#)

---

***Am besten abschalten: Alte NAS-Geräte von D-Link führen Fremdcode aus***

Der Hersteller D-Link bietet keine Patches für die veralteten NAS der ShareCenter-Serie mehr an. Betroffene sollten sie vom Internet trennen oder pensionieren.

- [Link](#)

---

***Patchday Adobe: Schadcode-Attacken auf Experience Manager & Co. möglich***

Adobe hat in mehreren Anwendungen kritische Sicherheitslücken geschlossen. Updates sollten zeitnah installiert werden.

- [Link](#)

---

***Patchday: Angreifer umgehen erneut Sicherheitsfunktion und attackieren Windows***

Microsoft hat wichtige Sicherheitsupdates für unter anderem Bitlocker, Office und Windows Defender veröffentlicht. Zwei Lücken nutzen Angreifer bereits aus.

- [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-2023-6895	0.901600000	0.987500000	<a href="#">Link</a>
CVE-2023-6553	0.916210000	0.988540000	<a href="#">Link</a>
CVE-2023-5360	0.967230000	0.996450000	<a href="#">Link</a>
CVE-2023-4966	0.964860000	0.995690000	<a href="#">Link</a>
CVE-2023-47246	0.934570000	0.990510000	<a href="#">Link</a>
CVE-2023-46805	0.965580000	0.996000000	<a href="#">Link</a>
CVE-2023-46747	0.971350000	0.997870000	<a href="#">Link</a>
CVE-2023-46604	0.972480000	0.998340000	<a href="#">Link</a>
CVE-2023-43177	0.960880000	0.994680000	<a href="#">Link</a>
CVE-2023-42793	0.970710000	0.997580000	<a href="#">Link</a>
CVE-2023-39143	0.938760000	0.990980000	<a href="#">Link</a>
CVE-2023-38646	0.928720000	0.989920000	<a href="#">Link</a>
CVE-2023-38203	0.967010000	0.996390000	<a href="#">Link</a>
CVE-2023-38035	0.973610000	0.998930000	<a href="#">Link</a>
CVE-2023-36845	0.966640000	0.996260000	<a href="#">Link</a>
CVE-2023-3519	0.911860000	0.988250000	<a href="#">Link</a>
CVE-2023-35082	0.947410000	0.992280000	<a href="#">Link</a>
CVE-2023-35078	0.965840000	0.996040000	<a href="#">Link</a>
CVE-2023-34993	0.944980000	0.991940000	<a href="#">Link</a>
CVE-2023-34960	0.938540000	0.990950000	<a href="#">Link</a>
CVE-2023-34634	0.925600000	0.989570000	<a href="#">Link</a>
CVE-2023-34362	0.960290000	0.994520000	<a href="#">Link</a>
CVE-2023-34039	0.907130000	0.987860000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3368	0.918440000	0.988780000	<a href="#">Link</a>
CVE-2023-33246	0.972820000	0.998500000	<a href="#">Link</a>
CVE-2023-32315	0.973670000	0.998960000	<a href="#">Link</a>
CVE-2023-32235	0.911650000	0.988210000	<a href="#">Link</a>
CVE-2023-30625	0.948330000	0.992450000	<a href="#">Link</a>
CVE-2023-30013	0.956380000	0.993830000	<a href="#">Link</a>
CVE-2023-29300	0.970480000	0.997460000	<a href="#">Link</a>
CVE-2023-29298	0.936290000	0.990720000	<a href="#">Link</a>
CVE-2023-28771	0.921620000	0.989040000	<a href="#">Link</a>
CVE-2023-28432	0.943220000	0.991560000	<a href="#">Link</a>
CVE-2023-28121	0.943690000	0.991640000	<a href="#">Link</a>
CVE-2023-27524	0.972950000	0.998560000	<a href="#">Link</a>
CVE-2023-27372	0.973490000	0.998880000	<a href="#">Link</a>
CVE-2023-27350	0.972040000	0.998120000	<a href="#">Link</a>
CVE-2023-26469	0.938630000	0.990960000	<a href="#">Link</a>
CVE-2023-26360	0.963530000	0.995310000	<a href="#">Link</a>
CVE-2023-26035	0.969280000	0.997050000	<a href="#">Link</a>
CVE-2023-25717	0.957880000	0.994060000	<a href="#">Link</a>
CVE-2023-25194	0.969270000	0.997050000	<a href="#">Link</a>
CVE-2023-2479	0.963600000	0.995340000	<a href="#">Link</a>
CVE-2023-24489	0.973920000	0.999100000	<a href="#">Link</a>
CVE-2023-23752	0.952140000	0.993030000	<a href="#">Link</a>
CVE-2023-23397	0.926450000	0.989680000	<a href="#">Link</a>
CVE-2023-23333	0.963260000	0.995240000	<a href="#">Link</a>
CVE-2023-22527	0.965680000	0.996030000	<a href="#">Link</a>
CVE-2023-22518	0.964830000	0.995660000	<a href="#">Link</a>
CVE-2023-22515	0.972680000	0.998400000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21839	0.958450000	0.994140000	<a href="#">Link</a>
CVE-2023-21554	0.959700000	0.994390000	<a href="#">Link</a>
CVE-2023-20887	0.962160000	0.994960000	<a href="#">Link</a>
CVE-2023-1671	0.967910000	0.996670000	<a href="#">Link</a>
CVE-2023-0669	0.969030000	0.996970000	<a href="#">Link</a>

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

Mon, 15 Apr 2024

#### **[NEU] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um Phishing-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Mon, 15 Apr 2024

#### **[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle in unbound**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um eine laufende Instanz zu manipulieren, Informationen offenzulegen oder einen Denial-of-Service auszulösen.

- [Link](#)

—

Fri, 12 Apr 2024

#### **[UPDATE] [hoch] Microsoft SQL Server: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft SQL Server 2019, Microsoft SQL Server 2022 und Microsoft SQL Server (MSSQL) ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 12 Apr 2024

#### **[NEU] [UNGEPATCHT] [hoch] ffmpeg: Schwachstelle ermöglicht Codeausführung und DoS**

Ein lokaler Angreifer kann eine Schwachstelle in ffmpeg ausnutzen, um beliebigen Programmcode



auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Thu, 11 Apr 2024

**[NEU] [hoch] Juniper Produkte: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Juniper Produkten ausnutzen um Denial of Service Zustände zu verursachen, Informationen offenzulegen und Sicherheitsmechanismen zu umgehen.

- [Link](#)

—

Thu, 11 Apr 2024

**[NEU] [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](#)

—

Thu, 11 Apr 2024

**[NEU] [hoch] GitLab: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Thu, 11 Apr 2024

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

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

- [Link](#)

—

Thu, 11 Apr 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um Dateien zu manipulieren, Daten offenzulegen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Thu, 11 Apr 2024

**[UPDATE] [hoch] QEMU: Schwachstelle ermöglicht Denial of Service und Codeausführung**

Ein lokaler Angreifer kann eine Schwachstelle in QEMU ausnutzen, um einen Denial of Service herbeizuführen und potenziell um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 11 Apr 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Thu, 11 Apr 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Thu, 11 Apr 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Thu, 11 Apr 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Thu, 11 Apr 2024

**[UPDATE] [hoch] util-linux: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein lokaler Angreifer kann eine Schwachstelle in util-linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Wed, 10 Apr 2024

**[NEU] [hoch] Paessler PRTG: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Paessler PRTG ausnutzen, um beliebigen Programmcode auszuführen einen Cross Site Scripting Angriff durchzuführen oder Informationen

offenzulegen.

- [Link](#)

—

Wed, 10 Apr 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 10 Apr 2024

**[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft 365 Apps, Microsoft Office, Microsoft SharePoint, Microsoft SharePoint Server 2016 und Microsoft SharePoint Server 2019 ausnutzen, um beliebigen Programmcode auszuführen oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—

Wed, 10 Apr 2024

**[NEU] [hoch] Microsoft Windows: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Windows 10, Microsoft Windows 11, Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019 und Microsoft Windows Server 2022 ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, beliebigen Programmcode mit Administratorrechten auszuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren

- [Link](#)

—

Wed, 10 Apr 2024

**[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder beliebigen Programmcode auszuführen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/15/2024	[PaperCut NG < 20.1.10 / 21.x < 21.2.14 / 22.x < 22.1.5 / 23.x < 23.0.7 Multiple Vulnerabilities]	critical
4/15/2024	[PaperCut MF < 20.1.10 / 21.x < 21.2.14 / 22.x < 22.1.5 / 23.x < 23.0.7 Multiple Vulnerabilities]	critical
4/15/2024	[VLC < 3.0.20 Multiple Vulnerabilities]	critical
4/14/2024	[Fedora 38 : kernel (2024-a56a47ef1b)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-45615)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-45616)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-35982)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-35980)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-45614)]	critical
4/13/2024	[Siemens Scalance W1750D Buffer Copy without Checking Size of Input (CVE-2023-35981)]	critical
4/15/2024	[Fedora 39 : chromium (2024-fe9a675a37)]	high
4/15/2024	[RHEL 8 : unbound (RHSA-2024:1804)]	high
4/15/2024	[RHEL 9 : bind and bind-dyndb-ldap security updates (Important) (RHSA-2024:1803)]	high
4/15/2024	[RHEL 9 : unbound (RHSA-2024:1801)]	high
4/15/2024	[RHEL 9 : bind and bind-dyndb-ldap security updates (Important) (RHSA-2024:1800)]	high
4/15/2024	[RHEL 8 : unbound (RHSA-2024:1802)]	high
4/15/2024	[Laravel Framework < 5.5.41 / 5.6.x < 5.6.30 RCE]	high

Datum	Schwachstelle	Bewertung
4/15/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : YARD vulnerabilities (USN-6731-1)]	high
4/15/2024	[FreeBSD : go – http2: close connections when receiving too many headers (cdb5e0e3-fafc-11ee-9c21-901b0e9408dc)]	high
4/15/2024	[Debian dla-3787 : xdmx - security update]	high
4/15/2024	[Ubuntu 22.04 LTS / 23.10 : WebKitGTK vulnerabilities (USN-6732-1)]	high
4/14/2024	[Fedora 38 : chromium (2024-f94660c56d)]	high
4/14/2024	[Fedora 39 : libopenmpt (2024-90b3798199)]	high
4/14/2024	[Fedora 38 : libopenmpt (2024-85b6c6fa92)]	high
4/14/2024	[Slackware Linux 15.0 / current less Vulnerability (SSA:2024-105-01)]	high
4/14/2024	[Debian dsa-5659 : trafficserver - security update]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45623)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45618)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45620)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45619)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45622)]	high
4/13/2024	[Siemens Scalance W1750D Improper Neutralization of Special Elements used in a Command (CVE-2023-45625)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45624)]	high
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45626)]	high

Datum	Schwachstelle	Bewertung
4/13/2024	[Siemens Scalance W1750D Improper Input Validation (CVE-2023-45617)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Mon, 15 Apr 2024

#### **Amazon AWS Glue Database Password Disclosure**

The password of database connections in AWS Glue is loaded into the website when a connection's edit page is requested. Principals with appropriate permissions can read the password. This behavior also increases the risk that database passwords will be intercepted by an attacker during transmission in the server response. Many types of vulnerabilities, such as broken access controls, cross site scripting and weaknesses in session handling, could enable an attacker to leverage this behavior to retrieve the passwords.

- [Link](#)

—

” “Mon, 15 Apr 2024

#### **CrushFTP Remote Code Execution**

This Metasploit exploit module leverages an improperly controlled modification of dynamically-determined object attributes vulnerability (CVE-2023-43177) to achieve unauthenticated remote code execution. This affects CrushFTP versions prior to 10.5.1. It is possible to set some user's session properties by sending an HTTP request with specially crafted Header key-value pairs. This enables an unauthenticated attacker to access files anywhere on the server file system and steal the session cookies of valid authenticated users. The attack consists in hijacking a user's session and escalates privileges to obtain full control of the target. Remote code execution is obtained by abusing the dynamic SQL driver loading and configuration testing feature.

- [Link](#)

—

” “Mon, 15 Apr 2024

#### **GLPI 10.x.x Remote Command Execution**

GLPI versions 10.x.x suffers from a remote command execution vulnerability via the shell commands plugin.

- [Link](#)

—

” “Mon, 15 Apr 2024

***WordPress WP Video Playlist 1.1.1 Cross Site Scripting***

WordPress WP Video Playlist plugin version 1.1.1 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

***BMC Compuware iStrobe Web 20.13 Shell Upload***

BMC Compuware iStrobe Web version 20.13 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

***Kruxton 1.0 SQL Injection***

Kruxton version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

***Kruxton 1.0 Shell Upload***

Kruxton version 1.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

***WBCE 1.6.0 SQL Injection***

WBCE version 1.6.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

***AMPLE BILLS 0.1 SQL injection***

AMPLE BILLS version 0.1 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

***PrusaSlicer 2.6.1 Arbitrary Code Execution***

PrusaSlicer versions 2.6.1 and below suffer from an arbitrary code execution vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

**Moodle 3.10.1 SQL Injection**

Moodle version 3.10.1 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

**Django REST Framework SimpleJWT 5.3.1 Information Disclosure**

Django REST Framework SimpleJWT versions 5.3.1 and below suffer from an information disclosure vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

**Jenkins 2.441 Local File Inclusion**

Jenkins version 2.441 suffers from a local file inclusion vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

**OpenClinic GA 5.247.01 Information Disclosure**

OpenClinic GA version 5.247.01 suffers from an information disclosure vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

**OpenClinic GA 5.247.01 Path Traversal**

OpenClinic GA version 5.247.01 suffers from an authenticated path traversal vulnerability.

- [Link](#)

—

” “Mon, 15 Apr 2024

**Online Fire Reporting System 1.2 SQL Injection**

Online Fire Reporting System version 1.2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 15 Apr 2024

**Stock Management System 1.0 SQL Injection**

Stock Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Fri, 12 Apr 2024

**Terratec dmx\_6fire USB 1.23.0.02 Unquoted Service Path**



Terratec dmx\_6fire USB version 1.23.0.02 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Fri, 12 Apr 2024

#### ***Ray OS 2.6.3 Command Injection***

The Ray Project dashboard contains a CPU profiling page, and the format parameter is not validated before being inserted into a system command executed in a shell, allowing for arbitrary command execution. If the system is configured to allow passwordless sudo (a setup some Ray configurations require) this will result in a root shell being returned to the user. If not configured, a user level shell will be returned. Versions 2.6.3 and below are affected.

- [Link](#)

—

” “Fri, 12 Apr 2024

#### ***WordPress Playlist For Youtube 1.32 Cross Site Scripting***

WordPress Playlist for Youtube plugin version 1.32 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 12 Apr 2024

#### ***MinIO Privilege Escalation***

MinIO versions prior to 2024-01-31T20-20-33Z suffer from a privilege escalation vulnerability.

- [Link](#)

—

” “Thu, 11 Apr 2024

#### ***Trimble TM4Web 22.2.0 Privilege Escalation / Access Code Disclosure***

An access control issue in Trimble TM4Web version 22.2.0 allows unauthenticated attackers to access a specific crafted URL path to retrieve the last registration access code and use this access code to register a valid account. If the access code was used to create an Administrator account, attackers are also able to register new Administrator accounts with full rights and privileges.

- [Link](#)

—

” “Thu, 11 Apr 2024

#### ***Concrete CMS 9.2.7 Cross Site Scripting / Open Redirect***

Concrete CMS version 9.2.7 suffers from information disclosure, open redirection, and persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 11 Apr 2024

**GUnet OpenEclass E-learning 3.15 File Upload / Command Execution**

GUnet OpenEclass E-learning platform version 3.15 suffers from an unrestricted file upload vulnerability in certbadge.php that allows for remote command execution.

- [Link](#)

—

” “Thu, 11 Apr 2024

**Windows Kernel Subkey List Use-After-Free**

The Windows Kernel suffers from a subkey list use-after-free vulnerability due to a mishandling of partial success in CmpAddSubKeyEx.

- [Link](#)

—

”

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

“Mon, 15 Apr 2024

**ZDI-24-367: (Pwn2Own) Google Chrome V8 Enum Cache Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 15 Apr 2024

**ZDI-24-366: (Pwn2Own) Google Chrome WASM Improper Input Validation Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 15 Apr 2024

**ZDI-24-365: (Pwn2Own) Microsoft Edge DOMArrayBuffer Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

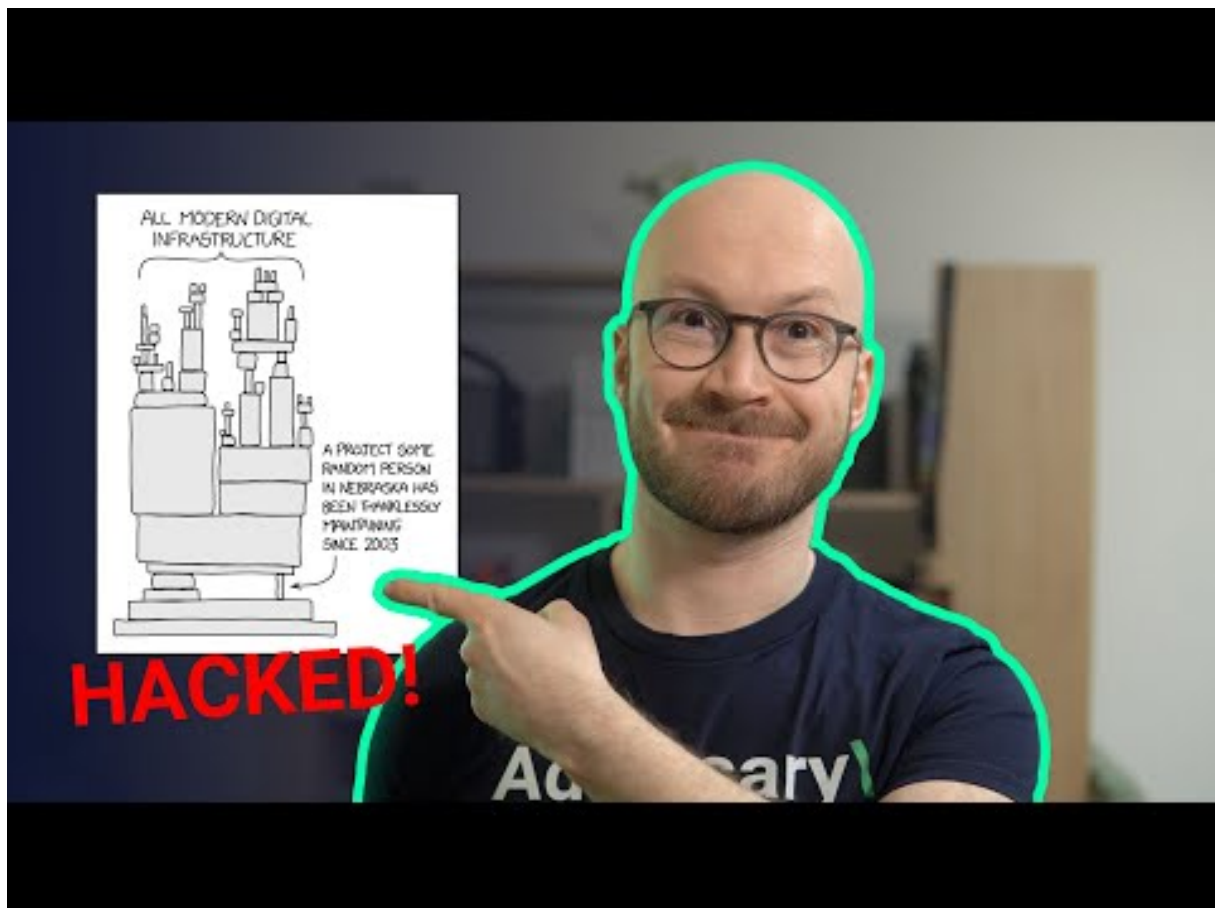
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Oh wow, this was very close: xz-utils was backdoored ☒



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information
2024-04-11	Taiwan United Renewable Energy Corporation (URECO)	[TWN]	<a href="#">Link</a>
2024-04-11	Swinomish Casino and Lodge	[USA]	<a href="#">Link</a>
2024-04-11	Iddink Learning Materials	[NLD]	<a href="#">Link</a>
2024-04-10	Ville de Saint-Nazaire et son agglomération	[FRA]	<a href="#">Link</a>
2024-04-09	The Heritage Foundation	[USA]	<a href="#">Link</a>
2024-04-09	Pak Suzuki	[PAK]	<a href="#">Link</a>
2024-04-07	CVS Group	[GBR]	<a href="#">Link</a>
2024-04-07	St. Elisabeth-Stiftung	[DEU]	<a href="#">Link</a>
2024-04-07	GBI-Genios Deutsche Wirtschaftsdatenbank GmbH	[DEU]	<a href="#">Link</a>
2024-04-05	Targus	[USA]	<a href="#">Link</a>
2024-04-04	Communauté de communes du bassin mussipontain	[FRA]	<a href="#">Link</a>
2024-04-04	Bielefeld Fertility Center	[DEU]	<a href="#">Link</a>
2024-04-03	New Mexico Highlands University	[USA]	<a href="#">Link</a>
2024-04-02	Comté de Jackson	[USA]	<a href="#">Link</a>
2024-04-02	Prepay Technologies	[ESP]	<a href="#">Link</a>
2024-04-02	Riley County	[USA]	<a href="#">Link</a>
2024-04-02	NorthBay Health	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-16	[UnivationTechnologies]	raworld	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-16	[Autoglass]	raworld	<a href="#">Link</a>
2024-04-16	[charlesparsons]	raworld	<a href="#">Link</a>
2024-04-16	[Cembell Industries]	qilin	<a href="#">Link</a>
2024-04-12	[Heritage Cooperative]	play	<a href="#">Link</a>
2024-04-15	[Druckman Law Group]	incransom	<a href="#">Link</a>
2024-04-15	[Pulaski academy]	incransom	<a href="#">Link</a>
2024-04-15	[Chicony Electronics]	hunters	<a href="#">Link</a>
2024-04-15	[Fullington Trailways]	dragonforce	<a href="#">Link</a>
2024-04-15	[bigtoe.yoga]	darkvault	<a href="#">Link</a>
2024-04-15	[regulatoremarine.com]	cactus	<a href="#">Link</a>
2024-04-15	[jeyesfluid.co.uk]	lockbit3	<a href="#">Link</a>
2024-04-15	[Deacon Jones]	dragonforce	<a href="#">Link</a>
2024-04-15	[Biggs Cardosa Associates]	blacksuit	<a href="#">Link</a>
2024-04-15	[The Post and Courier]	blacksuit	<a href="#">Link</a>
2024-04-15	[Best Reward Federal Credit Union]	akira	<a href="#">Link</a>
2024-04-15	[LYON TERMINAL]	8base	<a href="#">Link</a>
2024-04-15	[R.B. Woodcraft, Inc.]	8base	<a href="#">Link</a>
2024-04-15	[GPI Corporate]	8base	<a href="#">Link</a>
2024-04-15	[SOA Architecture]	8base	<a href="#">Link</a>
2024-04-15	[ASMFC: Atlantic States Marine Fisheries Commission]	8base	<a href="#">Link</a>
2024-04-15	[The Souza Agency Inc.]	8base	<a href="#">Link</a>
2024-04-15	[LEMODOR]	8base	<a href="#">Link</a>
2024-04-15	[Council for Relationships]	8base	<a href="#">Link</a>
2024-04-15	[compagniedephalsbourg.com]	threeam	<a href="#">Link</a>
2024-04-15	[ndpaper.com]	lockbit3	<a href="#">Link</a>
2024-04-14	[qint.com.br]	darkvault	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-14	[Jack Doheny Company]	hunters	<a href="#">Link</a>
2024-04-13	[Traverse City Area Public Schools ]	medusa	<a href="#">Link</a>
2024-04-14	[Omni Hotels & Resorts (US)]	daixin	<a href="#">Link</a>
2024-04-13	[countryvillahealth.com]	lockbit3	<a href="#">Link</a>
2024-04-13	[disb.dc.gov]	lockbit3	<a href="#">Link</a>
2024-04-09	[Williams County Abstract Company ]	medusa	<a href="#">Link</a>
2024-04-12	[Solano County Library ]	medusa	<a href="#">Link</a>
2024-04-12	[Alliance Mercantile]	medusa	<a href="#">Link</a>
2024-04-12	[Novus International]	medusa	<a href="#">Link</a>
2024-04-13	[Toyota Brazil]	hunters	<a href="#">Link</a>
2024-04-13	[Kablutronik SRL]	hunters	<a href="#">Link</a>
2024-04-13	[Caxton and CTP Publishers and Printers]	hunters	<a href="#">Link</a>
2024-04-13	[NanoLumens]	hunters	<a href="#">Link</a>
2024-04-13	[Integrated Control]	hunters	<a href="#">Link</a>
2024-04-13	[Frederick Wildman and Sons]	hunters	<a href="#">Link</a>
2024-04-12	[oraclecms.com]	lockbit3	<a href="#">Link</a>
2024-04-04	[thsp.co.uk]	darkvault	<a href="#">Link</a>
2024-04-12	[tommyclub.co.uk]	darkvault	<a href="#">Link</a>
2024-04-12	[Notions Marketing]	hunters	<a href="#">Link</a>
2024-04-12	[Jordano's Inc.]	hunters	<a href="#">Link</a>
2024-04-12	[Bojangles' International]	hunters	<a href="#">Link</a>
2024-04-12	[Snchez-Betances Sifre & Muñoz-Noya]	akira	<a href="#">Link</a>
2024-04-10	[Feldstein & Stewart]	play	<a href="#">Link</a>
2024-04-12	[Agate Construction]	play	<a href="#">Link</a>
2024-04-12	[H??????? C??????????]	play	<a href="#">Link</a>
2024-04-12	[Robeson County Sheriff's Office ]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-12	[MCP GROUP Commercial Contractor Topeka]	blacksuit	<a href="#">Link</a>
2024-04-12	[Hernando County]	rhysida	<a href="#">Link</a>
2024-04-11	[baheyabeauty.com]	darkvault	<a href="#">Link</a>
2024-04-11	[baheya.com]	darkvault	<a href="#">Link</a>
2024-04-12	[Oki Golf]	rhysida	<a href="#">Link</a>
2024-04-12	[Gimex]	raworld	<a href="#">Link</a>
2024-04-12	[Victor Fauconnier]	raworld	<a href="#">Link</a>
2024-04-11	[MoldTech]	play	<a href="#">Link</a>
2024-04-11	[Theatrixx Technologies]	play	<a href="#">Link</a>
2024-04-11	[Access Intelligence]	play	<a href="#">Link</a>
2024-04-11	[New England Wooden Ware]	play	<a href="#">Link</a>
2024-04-11	[LS Networks]	play	<a href="#">Link</a>
2024-04-11	[The MBTW Group]	play	<a href="#">Link</a>
2024-04-11	[Wencor.com]	cloak	<a href="#">Link</a>
2024-04-11	[Theharriscenter.org]	cloak	<a href="#">Link</a>
2024-04-11	[Community Alliance]	incransom	<a href="#">Link</a>
2024-04-11	[Henningson & Snoxell, Ltd.]	incransom	<a href="#">Link</a>
2024-04-11	[Optima Manufacturing]	hunters	<a href="#">Link</a>
2024-04-08	[wexer.com]	darkvault	<a href="#">Link</a>
2024-04-11	[Missouri Electric Cooperatives]	akira	<a href="#">Link</a>
2024-04-10	[F???s???? & ??????t]	play	<a href="#">Link</a>
2024-04-10	[Inszone Insurance Services]	hunters	<a href="#">Link</a>
2024-04-10	[Nexperia]	dunghill	<a href="#">Link</a>
2024-04-10	[Samart]	akira	<a href="#">Link</a>
2024-04-10	[Robertson Cheatham Farmers]	hunters	<a href="#">Link</a>
2024-04-10	[specialoilfield.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-09	[Consilux (Brazil)]	akira	<a href="#">Link</a>
2024-04-09	[processsolutions.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[numotion.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[siemensmfg.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[Parklane Group]	blackbasta	<a href="#">Link</a>
2024-04-09	[sermo.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[schlesingerlaw.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[robar.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[atlascontainer.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[patersoncooke.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[arch-con.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[New Production Concept]	dragonforce	<a href="#">Link</a>
2024-04-09	[Precision Pulley & Idler]	blacksuit	<a href="#">Link</a>
2024-04-09	[columbiapipe.com]	blackbasta	<a href="#">Link</a>
2024-04-09	[T A Khoury]	hunters	<a href="#">Link</a>
2024-04-09	[Kadushisoft]	dragonforce	<a href="#">Link</a>
2024-04-09	[Saint Cecilia's Church of England School]	dragonforce	<a href="#">Link</a>
2024-04-09	[Swansea & South Wales]	dragonforce	<a href="#">Link</a>
2024-04-09	[MajuHome Concept]	dragonforce	<a href="#">Link</a>
2024-04-09	[Team Locum]	dragonforce	<a href="#">Link</a>
2024-04-09	[Rigcon]	dragonforce	<a href="#">Link</a>
2024-04-09	[Vstblekinge Miljo]	dragonforce	<a href="#">Link</a>
2024-04-09	[JM Heaford]	blacksuit	<a href="#">Link</a>
2024-04-09	[Eagle Hydraulic Components]	blacksuit	<a href="#">Link</a>
2024-04-09	[MULTI-FILL]	blacksuit	<a href="#">Link</a>
2024-04-09	[Central Carolina Insurance Agency Inc.]	bianlian	<a href="#">Link</a>
2024-04-09	[Panacea Healthcare Services]	bianlian	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-09	[Baca County Feedyard, Inc]	ransomhub	<a href="#">Link</a>
2024-04-09	[Brewer & Company of WV]	blacksuit	<a href="#">Link</a>
2024-04-09	[Olea Kiosks]	blacksuit	<a href="#">Link</a>
2024-04-09	[Hudson Supplies]	blacksuit	<a href="#">Link</a>
2024-04-09	[Homeocan]	blacksuit	<a href="#">Link</a>
2024-04-09	[Macuz]	ciphbit	<a href="#">Link</a>
2024-04-09	[speditionlangen.de]	mallox	<a href="#">Link</a>
2024-04-09	[maccarinelli.it]	qilin	<a href="#">Link</a>
2024-04-08	[Skyway Coach Lines and Shuttle Services – skywaycoach.ca]	ransomhub	<a href="#">Link</a>
2024-04-08	[John R. Wood Properties ]	medusa	<a href="#">Link</a>
2024-04-08	[Paulmann Licht]	hunters	<a href="#">Link</a>
2024-04-08	[PGF Technology Group]	akira	<a href="#">Link</a>
2024-04-08	[REV Drill Sales & Rentals]	akira	<a href="#">Link</a>
2024-04-08	[PHARMACY ETTORE FLORIO SNC - Online Pharmacy Italy ]	ransomhub	<a href="#">Link</a>
2024-04-05	[Paducah Dermatology]	medusa	<a href="#">Link</a>
2024-04-05	[Domestic Violence Project, Inc]	medusa	<a href="#">Link</a>
2024-04-05	[Rairdon Automotive Group ]	medusa	<a href="#">Link</a>
2024-04-05	[Integration International ]	medusa	<a href="#">Link</a>
2024-04-06	[Tarrant Appraisal District ]	medusa	<a href="#">Link</a>
2024-04-08	[Speditionweise.de]	cloak	<a href="#">Link</a>
2024-04-08	[Mahoney Foundry, Inc.]	8base	<a href="#">Link</a>
2024-04-08	[DUNN, PITTMAN, SKINNER and CUSHMAN, PLLC]	8base	<a href="#">Link</a>
2024-04-08	[Inno-soft Info Systems Pte Ltd]	8base	<a href="#">Link</a>
2024-04-08	[Z Development Services, LLC]	8base	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-08	[Change HealthCare - OPTUM Group - United HealthCare Group]	ransomhub	<a href="#">Link</a>
2024-04-07	[PalauGov]	dragonforce	<a href="#">Link</a>
2024-04-07	[Ellsworth Cooperative Creamery]	blacksuit	<a href="#">Link</a>
2024-04-07	[SERVICES INFORMATIQUES POUR PROFESSIONNELS(SIP)]	blacksuit	<a href="#">Link</a>
2024-04-07	[Malaysian Industrial Development Finance]	rhysida	<a href="#">Link</a>
2024-04-07	[easchangesystems]	qilin	<a href="#">Link</a>
2024-04-06	[Carrozzeria Aretusa srl ]	ransomhub	<a href="#">Link</a>
2024-04-06	[HCI Systems, Inc. ]	ransomhub	<a href="#">Link</a>
2024-04-06	[Madero]	qilin	<a href="#">Link</a>
2024-04-06	[Chambers Construction]	bianlian	<a href="#">Link</a>
2024-04-06	[On Q Financial, LLC]	bianlian	<a href="#">Link</a>
2024-04-06	[Better Accounting Solutions ]	ransomhub	<a href="#">Link</a>
2024-04-06	[TermoPlastic S.R.L.]	ciphbit	<a href="#">Link</a>
2024-04-05	[truehomes.com]	lockbit3	<a href="#">Link</a>
2024-04-04	[Good Morning]	donutleaks	<a href="#">Link</a>
2024-04-05	[casio india]	stormous	<a href="#">Link</a>
2024-04-05	[emalon.co.il]	malekteam	<a href="#">Link</a>
2024-04-05	[Aussizz Group]	dragonforce	<a href="#">Link</a>
2024-04-05	[Doctorim]	malekteam	<a href="#">Link</a>
2024-04-05	[Agencia Host ]	ransomhub	<a href="#">Link</a>
2024-04-05	[Commerce Dental Group]	ciphbit	<a href="#">Link</a>
2024-04-04	[Sit]	play	<a href="#">Link</a>
2024-04-04	[Guy's Floor Service]	play	<a href="#">Link</a>
2024-04-04	[Everbrite]	play	<a href="#">Link</a>
2024-04-03	[Orientrose Contracts ]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-03	[Sutton Dental Arts]	medusa	<a href="#">Link</a>
2024-04-04	[Inspection Services]	akira	<a href="#">Link</a>
2024-04-04	[Radiant Canada]	akira	<a href="#">Link</a>
2024-04-04	[Constelacion Savings and Credit Society]	ransomhub	<a href="#">Link</a>
2024-04-04	[Remitano - Cryptocurrency Exchange]	incransom	<a href="#">Link</a>
2024-04-04	[mcalvain.com]	cactus	<a href="#">Link</a>
2024-04-03	[Precision Pulley & Idler]	blacksuit	<a href="#">Link</a>
2024-04-03	[Wacks Law Group]	qilin	<a href="#">Link</a>
2024-04-03	[BeneCare Dental Insurance]	hunters	<a href="#">Link</a>
2024-04-03	[Interface]	hunters	<a href="#">Link</a>
2024-04-03	[DataBank]	hunters	<a href="#">Link</a>
2024-04-03	[Beaver Run Resort]	hunters	<a href="#">Link</a>
2024-04-03	[Benetton Group]	hunters	<a href="#">Link</a>
2024-04-03	[Citi Trends]	hunters	<a href="#">Link</a>
2024-04-03	[Intersport]	hunters	<a href="#">Link</a>
2024-04-03	[West Idaho Orthopedics]	incransom	<a href="#">Link</a>
2024-04-03	[Norman Urology Associates]	incransom	<a href="#">Link</a>
2024-04-03	[Phillip Townsend Associates]	blacksuit	<a href="#">Link</a>
2024-04-02	[San Pasqual Band of Mission Indians]	medusa	<a href="#">Link</a>
2024-04-02	[East Baton Rouge Sheriff's Office]	medusa	<a href="#">Link</a>
2024-04-03	[Leicester City Council]	incransom	<a href="#">Link</a>
2024-04-03	[Ringhoffer Verzahnungstechnik GmbH and Co. KG]	8base	<a href="#">Link</a>
2024-04-03	[Samhwa Paint Ind. Ltd]	8base	<a href="#">Link</a>
2024-04-03	[Tamura Corporation]	8base	<a href="#">Link</a>
2024-04-03	[Apex Business Advisory]	8base	<a href="#">Link</a>
2024-04-03	[Pim]	8base	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-04-03	[Innomotive Systems Hainichen GmbH]	raworld	<a href="#">Link</a>
2024-04-03	[Seven Seas Technology]	rhysida	<a href="#">Link</a>
2024-04-01	[casajove.com]	lockbit3	<a href="#">Link</a>
2024-04-03	[delhipolice.gov.in]	killsec	<a href="#">Link</a>
2024-04-02	[regencyfurniture.com]	cactus	<a href="#">Link</a>
2024-04-02	[KICO GROUP]	raworld	<a href="#">Link</a>
2024-04-02	[GRUPOCREATIVO HERRERA]	qilin	<a href="#">Link</a>
2024-04-02	[Fincasrevuelta Data Leak]	everest	<a href="#">Link</a>
2024-04-02	[Precision Pulley & Idler]	blacksuit	<a href="#">Link</a>
2024-04-02	[W.P.J. McCarthy and Company]	qilin	<a href="#">Link</a>
2024-04-02	[Crimsgroup Data Leak]	everest	<a href="#">Link</a>
2024-04-02	[Gaia Herbs]	blacksuit	<a href="#">Link</a>
2024-04-02	[Sterling Plumbing Inc]	raworld	<a href="#">Link</a>
2024-04-02	[C&C Casa e Construção Ltda]	raworld	<a href="#">Link</a>
2024-04-02	[TUBEX Aluminium Tubes]	raworld	<a href="#">Link</a>
2024-04-01	[Roberson & Sons Insurance Services]	qilin	<a href="#">Link</a>
2024-04-01	[Partridge Venture Engineering]	blacksuit	<a href="#">Link</a>
2024-04-01	[anwaltskanzlei-kaufbeuren.de]	lockbit3	<a href="#">Link</a>
2024-04-01	[pdq-airspares.co.uk]	blackbasta	<a href="#">Link</a>
2024-04-01	[aerodynamicinc.com]	cactus	<a href="#">Link</a>
2024-04-01	[besttrans.com]	cactus	<a href="#">Link</a>
2024-04-01	[Xenwerx Initiatives, LLC]	incransom	<a href="#">Link</a>
2024-04-01	[Blueline Associates]	incransom	<a href="#">Link</a>
2024-04-01	[Sisu Healthcare]	incransom	<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.