

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240215



## 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 . . . . .	10
<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 AnyDesk-Hack und Jenkins-Lücke . . . . .	24
<b>6 Cyberangriffe: (Feb)</b>	<b>25</b>
<b>7 Ransomware-Erpressungen: (Feb)</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

#### **AMD meldet zahlreiche Sicherheitslücken in Prozessoren**

AMD hat Sicherheitsmitteilungen zu Schwachstellen in diversen Prozessoren veröffentlicht. Firmwareupdates sollen sie ausbessern.

- [Link](#)

---

#### **Webkonferenz-Tool Zoom: Rechteausweitung durch kritische Schwachstelle**

Zoom warnt vor mehreren Schwachstellen in den Produkten des Unternehmens. Eine gilt als kritisches Sicherheitsrisiko.

- [Link](#)

---

#### **Patchday: Adobe schließt Schadcode-Lücken in Acrobat & Co.**

Für mehrere Adobe-Produkte sind wichtige Sicherheitsupdates erschienen. Damit haben die Entwickler unter anderem kritische Schwachstellen geschlossen.

- [Link](#)

---

#### **Sicherheitslücke in Webmailer Roundcube wird angegriffen**

Angreifer attackieren eine Sicherheitslücke in dem Webmail-Programm Roundcube. Ein Update steht bereits länger bereit.

- [Link](#)

---

#### **Patchday: Attacken auf Windows - Sicherheitsfunktion SmartScreen umgangen**

Aufgrund von laufenden Attacken sollten Windows-Admins die aktuellen Sicherheitsupdates zügig installieren.

- [Link](#)

---

#### **DNS-Server: Bind, dnsmasq und Unbound stolpern über Sicherheitslücke "KeyTrap"**

Mit einer präparierten DNS-Anfrage können Angreifer eine hohe Prozessorlast verursachen und den Dienst für legitime Nutzer so blockieren. Patches stehen bereit.

- [Link](#)

---

#### **SAP: 13 neue Sicherheitswarnungen zum Februar-Patchday**

SAP verteilt Software-Updates, die Schwachstellen aus 13 Sicherheitsmitteilungen ausbessern. Eine Lücke ist kritisch.

- [Link](#)

---

---

***Sicherheitslücken: Angreifer können Dell Unity kompromittieren***

Dells Storage-Appliance-Serie Unity ist über mehrere Schwachstellen attackierbar. Sicherheitspatches sind verfügbar.

- [Link](#)

---

***Qnap: Sicherheitslücken in Firmware erlauben Einschleusen von Befehlen***

Qnap warnt vor Sicherheitslücken im Betriebssystem QTS, QuTS hero und QuTScloud. Angreifer aus dem Netz können dadurch Befehle einschmuggeln.

- [Link](#)

---

***PostgreSQL lässt sich beliebiges SQL unterjubeln***

Eine hochriskante Schwachstelle in der Datenbank PostgreSQL ermöglicht Angreifern, beliebige SQL-Befehle einzuschleusen.

- [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-2023-6553	0.909010000	0.987450000	<a href="#">Link</a>
CVE-2023-5360	0.967230000	0.996240000	<a href="#">Link</a>
CVE-2023-4966	0.966310000	0.995890000	<a href="#">Link</a>
CVE-2023-47246	0.943540000	0.991180000	<a href="#">Link</a>
CVE-2023-46805	0.962740000	0.994750000	<a href="#">Link</a>
CVE-2023-46747	0.971390000	0.997670000	<a href="#">Link</a>
CVE-2023-46604	0.972850000	0.998400000	<a href="#">Link</a>
CVE-2023-43177	0.932620000	0.989870000	<a href="#">Link</a>
CVE-2023-42793	0.973130000	0.998570000	<a href="#">Link</a>
CVE-2023-41265	0.915100000	0.987940000	<a href="#">Link</a>
CVE-2023-39143	0.920480000	0.988530000	<a href="#">Link</a>
CVE-2023-38205	0.932790000	0.989900000	<a href="#">Link</a>
CVE-2023-38035	0.974110000	0.999220000	<a href="#">Link</a>
CVE-2023-36845	0.964780000	0.995340000	<a href="#">Link</a>
CVE-2023-3519	0.912410000	0.987760000	<a href="#">Link</a>
CVE-2023-35082	0.962080000	0.994590000	<a href="#">Link</a>
CVE-2023-35078	0.952060000	0.992540000	<a href="#">Link</a>
CVE-2023-34960	0.931300000	0.989690000	<a href="#">Link</a>
CVE-2023-34634	0.919000000	0.988370000	<a href="#">Link</a>
CVE-2023-34362	0.961230000	0.994380000	<a href="#">Link</a>
CVE-2023-3368	0.928930000	0.989390000	<a href="#">Link</a>
CVE-2023-33246	0.973410000	0.998730000	<a href="#">Link</a>
CVE-2023-32315	0.973860000	0.999020000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32235	0.902020000	0.986930000	<a href="#">Link</a>
CVE-2023-30625	0.951530000	0.992410000	<a href="#">Link</a>
CVE-2023-30013	0.936180000	0.990180000	<a href="#">Link</a>
CVE-2023-29300	0.958470000	0.993780000	<a href="#">Link</a>
CVE-2023-28771	0.923800000	0.988900000	<a href="#">Link</a>
CVE-2023-28121	0.932010000	0.989740000	<a href="#">Link</a>
CVE-2023-27524	0.972220000	0.998100000	<a href="#">Link</a>
CVE-2023-27372	0.970420000	0.997260000	<a href="#">Link</a>
CVE-2023-27350	0.972270000	0.998140000	<a href="#">Link</a>
CVE-2023-26469	0.936750000	0.990270000	<a href="#">Link</a>
CVE-2023-26360	0.957020000	0.993500000	<a href="#">Link</a>
CVE-2023-26035	0.968710000	0.996700000	<a href="#">Link</a>
CVE-2023-25717	0.962730000	0.994730000	<a href="#">Link</a>
CVE-2023-2479	0.964780000	0.995340000	<a href="#">Link</a>
CVE-2023-24489	0.973640000	0.998860000	<a href="#">Link</a>
CVE-2023-23752	0.949820000	0.992130000	<a href="#">Link</a>
CVE-2023-23397	0.904540000	0.987050000	<a href="#">Link</a>
CVE-2023-22527	0.964800000	0.995350000	<a href="#">Link</a>
CVE-2023-22518	0.970760000	0.997370000	<a href="#">Link</a>
CVE-2023-22515	0.962730000	0.994740000	<a href="#">Link</a>
CVE-2023-21839	0.961800000	0.994520000	<a href="#">Link</a>
CVE-2023-21554	0.961220000	0.994370000	<a href="#">Link</a>
CVE-2023-20887	0.965640000	0.995700000	<a href="#">Link</a>
CVE-2023-20198	0.919220000	0.988390000	<a href="#">Link</a>
CVE-2023-1671	0.964220000	0.995210000	<a href="#">Link</a>
CVE-2023-0669	0.968020000	0.996510000	<a href="#">Link</a>

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

Wed, 14 Feb 2024

**[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.

- [Link](#)

—

Wed, 14 Feb 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, 14 Feb 2024

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

Ein Angreifer kann mehrere Schwachstellen in Xen ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 14 Feb 2024

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

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

- [Link](#)

—

Wed, 14 Feb 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 14 Feb 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, 14 Feb 2024

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

Ein Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Office Anwendungen ausnutzen, um beliebigen Code auszuführen, seine Privilegien zu eskalieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 14 Feb 2024

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

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Informationen falsch darzustellen.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Zoom Video Communications Zoom Client: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Zoom Video Communications Zoom Client ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen oder seine Berechtigungen zu erweitern.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Adobe Magento: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Adobe Magento ausnutzen, um Cross-Site-Scripting (XSS)-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Adobe Acrobat: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe Acrobat, Adobe Acrobat Reader, Adobe Acrobat DC und Adobe Acrobat Reader DC ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder Informationen offenzulegen.

- [Link](#)

—  
Wed, 14 Feb 2024

**[NEU] [hoch] Microsoft Dynamics 365: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Microsoft Dynamics 365 ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Intel Driver and Support Assistant: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Driver and Support Assistant ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Microsoft GitHub Enterprise: Mehrere Schwachstellen ermöglichen Privilegieneskalation**

Ein entfernter Angreifer kann mehrere Schwachstellen in Microsoft GitHub Enterprise ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Intel Thunderbolt DCH Drivers: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Thunderbolt DCH-Treibern ausnutzen, um vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen oder seine Berechtigungen zu erweitern.

- [Link](#)

—

Wed, 14 Feb 2024

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

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und Daten falsch darzustellen.

- [Link](#)

—

Wed, 14 Feb 2024

**[NEU] [hoch] Adobe FrameMaker: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Adobe FrameMaker ausnutzen, um

Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Wed, 14 Feb 2024

**[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen und Daten zu manipulieren.

- [Link](#)

—

Wed, 14 Feb 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](#)

—

Wed, 14 Feb 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/14/2024	[Fedora 38 : firecracker / libkrun / rust-event-manager / rust-kvm-bindings / etc (2024-f2305d485f)]	critical
2/14/2024	[Ubuntu 22.04 LTS : Linux kernel (GCP) vulnerabilities (USN-6635-1)]	critical

Datum	Schwachstelle	Bewertung
2/14/2024	[Fedora 39 : clamav (2024-3439911df6)]	high
2/14/2024	[Cisco Secure Endpoint DoS (cisco-sa-clamav-dos-FTkhqMWZ)]	high
2/14/2024	[Debian dsa-5620 : libunbound-dev - security update]	high
2/14/2024	[Debian dsa-5621 : bind9 - security update]	high
2/14/2024	[PostgreSQL 12.x < 12.18 / 13.x < 13.14 / 14.x < 14.11 / 15.x < 15.6 SQL Injection]	high
2/14/2024	[AlmaLinux 9 : sudo (ALSA-2024:0811)]	high
2/14/2024	[RHEL 7 : .NET 6.0 (RHSA-2024:0814)]	high
2/14/2024	[RHEL 8 / 9 : sudo (RHSA-2024:0811)]	high
2/14/2024	[Ubuntu 22.04 LTS : Linux kernel vulnerabilities (USN-6626-2)]	high
2/14/2024	[Ubuntu 22.04 LTS : Linux kernel (NVIDIA) vulnerabilities (USN-6608-2)]	high
2/14/2024	[Slackware Linux 15.0 / current dnsmasq Multiple Vulnerabilities (SSA:2024-044-02)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP Advanced WAF and BIG-IP ASM vulnerability (K000137416)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP SSL Client Certificate LDAP and CRLDP Authentication profiles vulnerability (K000134516)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP PEM vulnerability (K000135946)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP TMM vulnerability (K000137333)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP Advanced WAF and BIG-IP ASM and vulnerability (K000137270)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP iControl REST vulnerability (K000137522)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP HTTP/2 vulnerability (K000137675)]	high

Datum	Schwachstelle	Bewertung
2/14/2024	[F5 Networks BIG-IP : BIG-IP AFM signature matching vulnerability (K000137595)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP iControl REST API vulnerability (K32544615)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP Websockets vulnerability (K000135873)]	high
2/14/2024	[Security Update for Microsoft .NET Core (February 2024)]	high
2/14/2024	[Oracle Linux 8 / 9 : sudo (ELSA-2024-0811)]	high
2/14/2024	[Oracle Linux 8 : container-tools:ol8 (ELSA-2024-0752)]	high
2/14/2024	[F5 Networks BIG-IP : F5 Application Visibility and Reporting module and BIG-IP Advanced WAF/ASM vulnerability (K000137334)]	high
2/14/2024	[F5 Networks BIG-IP : BIG-IP AFM vulnerability (K000137521)]	high
2/14/2024	[Security Updates for Microsoft Office Products C2R (February 2024)]	high
2/14/2024	[Security Updates for Microsoft Visio Products C2R (August 2023)]	high
2/14/2024	[Security Updates for Outlook C2R (February 2024)]	high
2/14/2024	[Security Updates for Microsoft Word Products C2R (February 2024)]	high
2/14/2024	[Security Update for Microsoft ASP.NET Core (February 2023) (CVE-2024-21386)]	high
2/14/2024	[Security Updates for Microsoft Dynamics 365 Business Central (February 2024)]	high
2/14/2024	[Security Updates for Microsoft Dynamics 365 (on-premises) (February 2024)]	high
2/14/2024	[Security Updates for Microsoft Visual Studio Products (February 2024)]	high
2/14/2024	[Bosch Security Systems B426 Conettix Improper Access Control (CVE-2021-23845)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Wed, 14 Feb 2024

#### ***Statamic CMS Cross Site Scripting***

Statamic CMS versions prior to 4.46.0 and 3.4.17 suffer from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Wed, 14 Feb 2024

#### ***Adapt CMS 3.0.3 Cross Site Scripting / Shell Upload***

Adapt CMS version 3.0.3 suffers from persistent cross site scripting and remote shell upload vulnerabilities.

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***XoopsCore25 2.5.11 Cross Site Scripting***

XoopsCore25 version 2.5.11 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***ManageEngine ADManager Plus Recovery Password Disclosure***

ManageEngine ADManager Plus versions prior to build 7183 suffers from a recovery password disclosure vulnerability.

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***Splunk 9.0.4 Information Disclosure***

Splunk version 9.0.4 suffers from an information disclosure vulnerability.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***LaborOfficeFree 19.10 MySQL Root Password Calculator***

LaborOfficeFree installs a MySQL instance that runs as SYSTEM and calculates the MySQL root password based on two constants. Each time the program needs to connect to MySQL as root, it employs the reverse algorithm to calculate the root password. This issue has been tested on version 19.10 exclusively, but allegedly, versions prior to 19.10 are also vulnerable.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***Windows Defender Detection Mitigation Bypass***

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***WyreStorm Apollo VX20 Incorrect Access Control***

An issue was discovered on WyreStorm Apollo VX20 versions prior to 1.3.58. Remote attackers can restart the device via a /device/reboot HTTP GET request.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***WyreStorm Apollo VX20 Credential Disclosure***

WyreStorm Apollo VX20 versions prior to 1.3.58 suffer from a cleartext credential disclosure vulnerability when accessing /device/config with an HTTP GET.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***WyreStorm Apollo VX20 Account Enumeration***

An issue was discovered on WyreStorm Apollo VX20 devices prior to version 1.3.58. The TELNET service prompts for a password only after a valid username is entered. Attackers who can reach the Apollo VX20 Telnet service can determine valid accounts allowing for account discovery.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***Enpass Desktop Application 6.9.2 HTML Injection***

Enpass Desktop Application version 6.9.2 suffers from an html injection vulnerability.

- [Link](#)

—

” “Mon, 12 Feb 2024

#### ***Complaint Management System 2.0 SQL Injection***

Complaint Management System version 2.0 suffers from multiple remote SQL injection vulnerabilities.

- [Link](#)

—

” “Mon, 12 Feb 2024

***SCHLIX 2.2.8-1 Denial Of Service***

SCHLIX version 2.2.8-1 suffers from a REGEX processing denial of service vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

***IBM i Access Client Solutions Remote Credential Theft***

IBM i Access Client Solutions (ACS) versions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.4 suffer from a remote credential theft vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

***Advanced Page Visit Counter 1.0 Cross Site Scripting***

Advanced Page Visit Counter version 1.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

***Online Nurse Hiring System 1.0 SQL Injection***

Online Nurse Hiring System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

***Rail Pass Management System 1.0 SQL Injection***

Rail Pass Management System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

” “Fri, 09 Feb 2024

***WordPress Augmented-Reality Remote Code Execution***

WordPress Augmented-Reality plugin suffers from a remote code execution vulnerability. It is unclear which versions are affected.

- [Link](#)

—

” “Fri, 09 Feb 2024

***WordPress Seotheme Shell Upload***

WordPress Seotheme plugin suffers from a remote shell upload vulnerability. It is unclear which



versions are affected.

- [Link](#)

---

” “Fri, 09 Feb 2024

#### ***Zyxel zysh Format String Proof Of Concept***

Proof of concept format string exploit for Zyxel zysh. Multiple improper input validation flaws were identified in some CLI commands of Zyxel USG/ZyWALL series firmware versions 4.09 through 4.71, USG FLEX series firmware versions 4.50 through 5.21, ATP series firmware versions 4.32 through 5.21, VPN series firmware versions 4.30 through 5.21, NSG series firmware versions 1.00 through 1.33 Patch 4, NXC2500 firmware version 6.10(AAIG.3) and earlier versions, NAP203 firmware version 6.25(ABFA.7) and earlier versions, NWA50AX firmware version 6.25(ABYW.5) and earlier versions, WAC500 firmware version 6.30(ABVS.2) and earlier versions, and WAX510D firmware version 6.30(ABTF.2) and earlier versions, that could allow a local authenticated attacker to cause a buffer overflow or a system crash via a crafted payload.

- [Link](#)

---

” “Thu, 08 Feb 2024

#### ***KiTTY 0.76.1.13 Buffer Overflows***

KiTTY versions 0.76.1.13 and below suffer from buffer overflows related to ANSI escape sequences. Two exploits are included as proof of concepts as well as a full documented breakdown of the issues.

- [Link](#)

---

” “Thu, 08 Feb 2024

#### ***KiTTY 0.76.1.13 Command Injection***

KiTTY versions 0.76.1.13 and below suffer from a command injection vulnerability when getting a remote file through scp. It appears to leverage an ANSI escape sequence issue which is quite an interesting vector of attack.

- [Link](#)

---

” “Thu, 08 Feb 2024

#### ***MediaTek WLAN Driver Memory Corruption***

The MediaTek WLAN driver has VFS read handlers that do not check buffer size leading to userland memory corruption.

- [Link](#)

---

” “Mon, 05 Feb 2024

#### ***Cacti pollers.php SQL Injection / Remote Code Execution***

This Metasploit exploit module leverages sql injection and local file inclusion vulnerabilities in

Cacti versions prior to 1.2.26 to achieve remote code execution. Authentication is needed and the account must have access to the vulnerable PHP script (pollers.php). This is granted by setting the Sites/Devices/Data permission in the General Administration section.

- [Link](#)

—

” “Mon, 05 Feb 2024

#### ***runc 1.1.11 File Descriptor Leak Privilege Escalation***

runc versions 1.1.11 and below, as used by containerization technologies such as Docker engine and Kubernetes, are vulnerable to an arbitrary file write vulnerability. Due to a file descriptor leak it is possible to mount the host file system with the permissions of runc (typically root). Successfully tested on Ubuntu 22.04 with runc 1.1.7-0ubuntu1~22.04.1 using Docker build.

- [Link](#)

—

”

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

“Tue, 13 Feb 2024

#### ***ZDI-24-169: Adobe Audition AVI File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***ZDI-24-168: Adobe Acrobat Pro DC Annotation Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***ZDI-24-167: Adobe Acrobat Pro DC AcroForm Use-After-Free Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***ZDI-24-166: Adobe Acrobat Pro DC AcroForm Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Tue, 13 Feb 2024

#### ***ZDI-24-165: Microsoft Windows Internet Shortcut SmartScreen Bypass Vulnerability***

- [Link](#)

—

” “Tue, 13 Feb 2024

***ZDI-24-164: Microsoft Office Word PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-163: (0Day) Autodesk AutoCAD STP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-162: (0Day) Autodesk AutoCAD X\_T File Parsing Untrusted Pointer Dereference Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-161: (0Day) Autodesk AutoCAD CATPART File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-160: (0Day) Autodesk AutoCAD STP File Parsing Untrusted Pointer Dereference Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-159: (0Day) Autodesk AutoCAD SLDPRD File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-158: (0Day) Autodesk AutoCAD IGES File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-157: (0Day) Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-156: (0Day) Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-155: (0Day) Autodesk AutoCAD IGS File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-154: (0Day) Autodesk AutoCAD STP File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-153: (0Day) Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-152: (0Day) Autodesk AutoCAD STP File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-151: (0Day) Autodesk AutoCAD STP File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

**ZDI-24-150: (0Day) Autodesk AutoCAD SLDPRT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-149: (0Day) Autodesk AutoCAD SLDASM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-148: (0Day) Autodesk AutoCAD 3DM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-147: (0Day) Autodesk AutoCAD CATPART File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-146: (0Day) Autodesk AutoCAD STP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-145: (0Day) Autodesk AutoCAD SLDASM File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-144: (0Day) Autodesk AutoCAD 3DM File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-143: (0Day) Autodesk AutoCAD MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-142: (0Day) Autodesk AutoCAD SLDPRT File Parsing Uninitialized Variable Remote Code***

**Execution Vulnerability**

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-141: (0Day) Autodesk AutoCAD STP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-140: (0Day) Autodesk AutoCAD MODEL File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-139: (0Day) Autodesk AutoCAD SLDASM File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-138: (0Day) Autodesk AutoCAD SLDASM File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-137: (0Day) Autodesk AutoCAD SLDASM File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-136: (0Day) Autodesk AutoCAD MODEL File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-135: (0Day) Autodesk AutoCAD STP File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-134: (0Day) Autodesk AutoCAD STP File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-133: (0Day) Autodesk AutoCAD SLDPRt File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-132: (0Day) Autodesk AutoCAD 3DM File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-131: (0Day) Autodesk AutoCAD CATPART File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-130: (0Day) Autodesk AutoCAD STEP File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-129: (0Day) Autodesk AutoCAD MODEL File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-128: (0Day) Autodesk AutoCAD MODEL File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-127: (0Day) Autodesk AutoCAD SLDPRt File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-126: (0Day) Autodesk AutoCAD STP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-125: (0Day) Autodesk AutoCAD MODEL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Mon, 12 Feb 2024

***ZDI-24-124: (0Day) Autodesk AutoCAD STP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

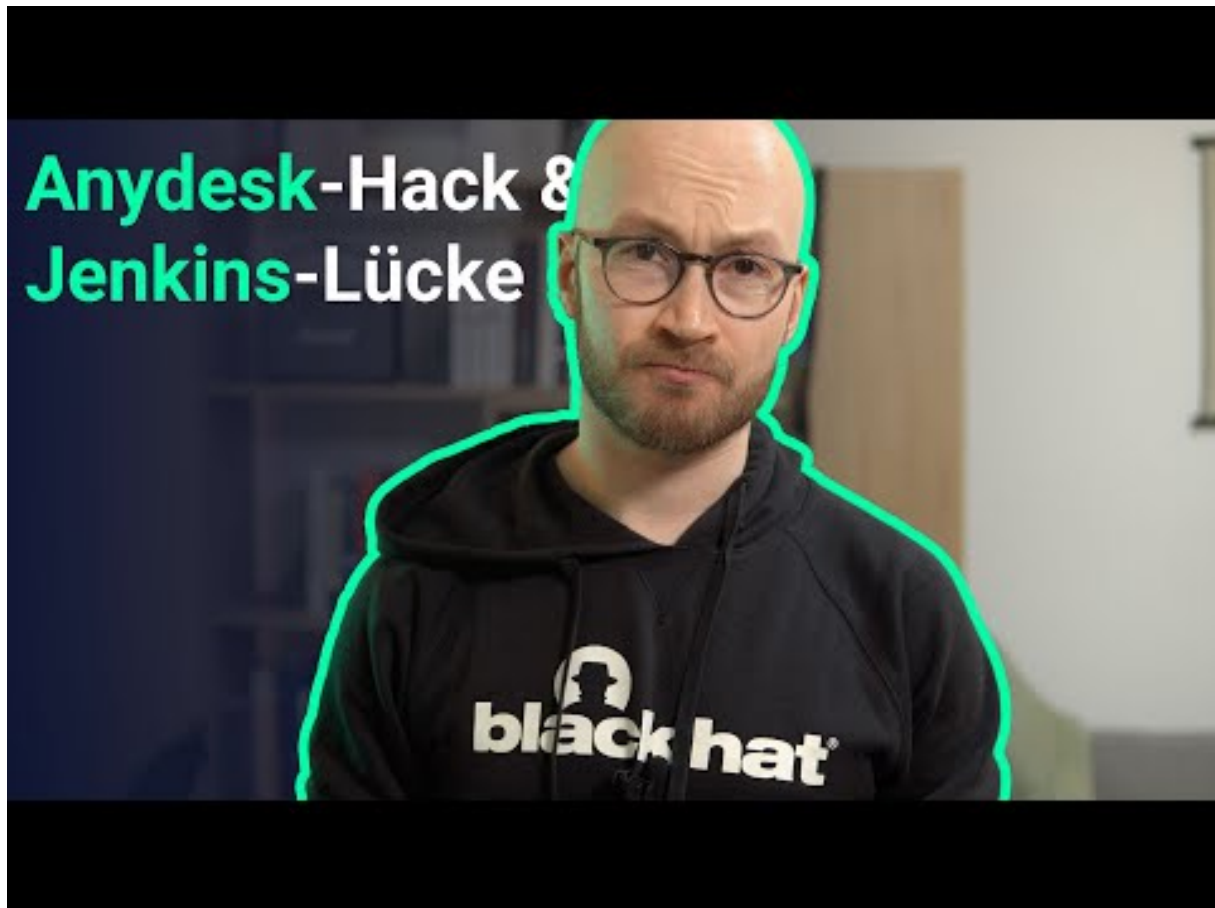
”



## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 AnyDesk-Hack und Jenkins-Lücke



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-13	Aztech Global	[SGP]	<a href="#">Link</a>
2024-02-13	Varta	[DEU]	<a href="#">Link</a>
2024-02-13	Coeur d'Alene	[USA]	<a href="#">Link</a>
2024-02-13	Act21	[FRA]	<a href="#">Link</a>
2024-02-12	MSH International	[CAN]	<a href="#">Link</a>
2024-02-11	Centre hospitalier d'Armentières	[FRA]	<a href="#">Link</a>
2024-02-11	Hipocrate Information System (HIS)	[ROU]	<a href="#">Link</a>
2024-02-11	Clinique privée La Colline (groupe Hirslanden)	[CHE]	<a href="#">Link</a>
2024-02-09	Office of Colorado State Public Defender	[USA]	<a href="#">Link</a>
2024-02-07	Université de Central Missouri	[USA]	<a href="#">Link</a>
2024-02-07	SouthState Bank	[USA]	<a href="#">Link</a>
2024-02-07	Commune de Petersberg	[DEU]	<a href="#">Link</a>
2024-02-07	Krankenhaus Lindenbrunn	[DEU]	<a href="#">Link</a>
2024-02-06	Commune de Kalmar	[SWE]	<a href="#">Link</a>
2024-02-06	Advania	[SWE]	<a href="#">Link</a>
2024-02-06	Onclusive	[GBR]	<a href="#">Link</a>
2024-02-05	Prudential Financial, Inc.	[USA]	<a href="#">Link</a>
2024-02-04	Northern Light Health	[USA]	<a href="#">Link</a>
2024-02-04	Middletown Area School District	[USA]	<a href="#">Link</a>
2024-02-02	Germantown	[USA]	<a href="#">Link</a>
2024-02-02	Université de Reykjavík	[ISL]	<a href="#">Link</a>
2024-02-02	Hôpital de la Trinité à Lippstadt, ainsi que les cliniques associées à Erwitte et Geseke.	[DEU]	<a href="#">Link</a>
2024-02-02	Mairie de Korneuburg	[AUT]	<a href="#">Link</a>
2024-02-01	Landkreis Kelheim	[DEU]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-02-01	Groton Public Schools	[USA]	<a href="#">Link</a>
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	<a href="#">Link</a>
2024-02-01	Ajuntament de Sant Antoni de Portmany	[ESP]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-14	[studiogalbusera.com]	lockbit3	<a href="#">Link</a>
2024-02-14	[Nekoosa School District]	akira	<a href="#">Link</a>
2024-02-14	[BM Catalysts bmcatalysts.co.uk]	mydata	<a href="#">Link</a>
2024-02-14	[vanwingerden.com]	abyss	<a href="#">Link</a>
2024-02-14	[KALEEDS]	qilin	<a href="#">Link</a>
2024-02-14	[conseguros]	qilin	<a href="#">Link</a>
2024-02-14	[kabat.pl]	lockbit3	<a href="#">Link</a>
2024-02-13	[Sindicato de Enfermería (SATSE)]	hunters	<a href="#">Link</a>
2024-02-13	[wsnelson.com]	lockbit3	<a href="#">Link</a>
2024-02-13	[fultoncountyga.gov]	lockbit3	<a href="#">Link</a>
2024-02-14	[UNIFER]	8base	<a href="#">Link</a>
2024-02-14	[Institutional Casework, Inc]	8base	<a href="#">Link</a>
2024-02-14	[ATB SA Ingénieurs-conseils SIA]	8base	<a href="#">Link</a>
2024-02-14	[mmiculinary.com]	lockbit3	<a href="#">Link</a>
2024-02-12	[adioscancer.com]	lockbit3	<a href="#">Link</a>
2024-02-14	[giraud]	qilin	<a href="#">Link</a>
2024-02-13	[rajawali.com]	lockbit3	<a href="#">Link</a>
2024-02-13	[motilaloswal.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-13	[barberemerson.com]	blackbasta	<a href="#">Link</a>
2024-02-13	[ffpkg.co.uk]	blackbasta	<a href="#">Link</a>
2024-02-13	[patriziapepe.com]	blackbasta	<a href="#">Link</a>
2024-02-13	[btl.info]	blackbasta	<a href="#">Link</a>
2024-02-13	[globalrescue.com]	blackbasta	<a href="#">Link</a>
2024-02-13	[ssmnlaw.com]	blackbasta	<a href="#">Link</a>
2024-02-13	[leonardssyrups.com]	blackbasta	<a href="#">Link</a>
2024-02-13	[ROOSENS BÉTONS]	qilin	<a href="#">Link</a>
2024-02-13	[universalservicesms.com]	lockbit3	<a href="#">Link</a>
2024-02-13	[Communication Federal Credit Union]	hunters	<a href="#">Link</a>
2024-02-13	[doprastav.sk]	lockbit3	<a href="#">Link</a>
2024-02-13	[The Source]	alphv	<a href="#">Link</a>
2024-02-13	[ArcisGolf]	alphv	<a href="#">Link</a>
2024-02-13	[Trans-Northern Pipelines]	alphv	<a href="#">Link</a>
2024-02-13	[Herrs]	alphv	<a href="#">Link</a>
2024-02-13	[Procopio]	alphv	<a href="#">Link</a>
2024-02-13	[New Indy Containerboard]	alphv	<a href="#">Link</a>
2024-02-13	[auruminstitute.org]	lockbit3	<a href="#">Link</a>
2024-02-10	[SOPEM]	hunters	<a href="#">Link</a>
2024-02-13	[Satse]	hunters	<a href="#">Link</a>
2024-02-13	[Sanok Rubber CompanySpółka Akcyjna]	akira	<a href="#">Link</a>
2024-02-12	[garonproducts.com]	threeam	<a href="#">Link</a>
2024-02-07	[tecasrl.it]	lockbit3	<a href="#">Link</a>
2024-02-12	[Antunovich Associates]	blacksuit	<a href="#">Link</a>
2024-02-12	[DHX–Dependable Hawaiian Express]	knight	<a href="#">Link</a>
2024-02-12	[Forgepresion.com]	cloak	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-12	[Rush Energy Services Inc [You have 48 hours]]	alphv	<a href="#">Link</a>
2024-02-12	[SERCIDE]	alphv	<a href="#">Link</a>
2024-02-12	[Lower Valley Energy, Inc]	alphv	<a href="#">Link</a>
2024-02-12	[Modern Kitchens ]	medusa	<a href="#">Link</a>
2024-02-12	[vhprimary.com]	lockbit3	<a href="#">Link</a>
2024-02-12	[germaintoiture.fr]	lockbit3	<a href="#">Link</a>
2024-02-12	[Disaronno International]	meow	<a href="#">Link</a>
2024-02-12	[Allmetal Inc.]	meow	<a href="#">Link</a>
2024-02-12	[Freedom Munitions]	meow	<a href="#">Link</a>
2024-02-12	[Arlington Perinatal Associates]	meow	<a href="#">Link</a>
2024-02-12	[jacksonvillebeach.org]	lockbit3	<a href="#">Link</a>
2024-02-12	[robs.org]	lockbit3	<a href="#">Link</a>
2024-02-12	[parkhomeassist.co.uk]	lockbit3	<a href="#">Link</a>
2024-02-12	[grotonschoools.org]	lockbit3	<a href="#">Link</a>
2024-02-12	[isspol.gov]	lockbit3	<a href="#">Link</a>
2024-02-12	[lyon.co.uk]	lockbit3	<a href="#">Link</a>
2024-02-12	[dienerprecisionpumps.com]	lockbit3	<a href="#">Link</a>
2024-02-12	[envie.org]	lockbit3	<a href="#">Link</a>
2024-02-12	[sealco-leb.com]	lockbit3	<a href="#">Link</a>
2024-02-12	[camarotto.it]	lockbit3	<a href="#">Link</a>
2024-02-12	[paltertonprimary.co.uk]	lockbit3	<a href="#">Link</a>
2024-02-12	[fidcornelis.be]	lockbit3	<a href="#">Link</a>
2024-02-12	[plexustelerad.com]	lockbit3	<a href="#">Link</a>
2024-02-12	[cabc.com.ar]	lockbit3	<a href="#">Link</a>
2024-02-12	[textiles.org.tw]	lockbit3	<a href="#">Link</a>
2024-02-12	[silverairways.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-12	[Kreyenhop & Kluge]	hunters	<a href="#">Link</a>
2024-02-12	[Kadac Australia]	medusa	<a href="#">Link</a>
2024-02-11	[Amoskeag Network Consulting Group LLC]	medusa	<a href="#">Link</a>
2024-02-11	[lacolline-skincare.com]	lockbit3	<a href="#">Link</a>
2024-02-10	[Upper Merion Township]	qilin	<a href="#">Link</a>
2024-02-10	[YKP LTDA]	ransomhub	<a href="#">Link</a>
2024-02-10	[Village of Skokie]	hunters	<a href="#">Link</a>
2024-02-10	[Lancaster County Sheriff's Office]	hunters	<a href="#">Link</a>
2024-02-10	[Nastech]	hunters	<a href="#">Link</a>
2024-02-10	[Benchmark Management Group]	hunters	<a href="#">Link</a>
2024-02-10	[SOPEM Tunisie]	hunters	<a href="#">Link</a>
2024-02-10	[Impact Energy Services]	hunters	<a href="#">Link</a>
2024-02-10	[Groupe Goyette]	hunters	<a href="#">Link</a>
2024-02-10	[Dalmahoy Hotel & Country Club]	hunters	<a href="#">Link</a>
2024-02-10	[Carespring Health Care]	hunters	<a href="#">Link</a>
2024-02-10	[Avianor Aircraft]	hunters	<a href="#">Link</a>
2024-02-10	[mranet.org]	abyss	<a href="#">Link</a>
2024-02-10	[aisg-online.com]	lockbit3	<a href="#">Link</a>
2024-02-10	[maddockhenson]	alphv	<a href="#">Link</a>
2024-02-10	[verdimed.es]	lockbit3	<a href="#">Link</a>
2024-02-10	[Pacific American Fish Company Inc.]	incransom	<a href="#">Link</a>
2024-02-09	[water.cc]	lockbit3	<a href="#">Link</a>
2024-02-09	[CTSI]	bianlian	<a href="#">Link</a>
2024-02-09	[J.P. Original]	bianlian	<a href="#">Link</a>
2024-02-09	[TechNet Kronoberg AB]	bianlian	<a href="#">Link</a>
2024-02-09	[Capozzi Adler, P.C.]	bianlian	<a href="#">Link</a>
2024-02-09	[Drost Kivlahan McMahon & O'Connor LLC]	bianlian	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-09	[Grace Lutheran Foundation]	alphv	<a href="#">Link</a>
2024-02-09	[ZGEO]	qilin	<a href="#">Link</a>
2024-02-09	[alfiras.com]	lockbit3	<a href="#">Link</a>
2024-02-09	[wannago.cloud]	qilin	<a href="#">Link</a>
2024-02-09	[grupomoraval.com]	lockbit3	<a href="#">Link</a>
2024-02-09	[cdtmedicus.pl]	lockbit3	<a href="#">Link</a>
2024-02-09	[soken-ce.co.jp]	lockbit3	<a href="#">Link</a>
2024-02-09	[maximumresearch.com]	lockbit3	<a href="#">Link</a>
2024-02-09	[indoramaventures.com]	lockbit3	<a href="#">Link</a>
2024-02-09	[willislease.com]	blackbasta	<a href="#">Link</a>
2024-02-09	[northseayachtsupport.nl]	lockbit3	<a href="#">Link</a>
2024-02-09	[seymourct.org]	lockbit3	<a href="#">Link</a>
2024-02-09	[bsaarchitects.com]	lockbit3	<a href="#">Link</a>
2024-02-09	[moneyadvicetrust.org]	lockbit3	<a href="#">Link</a>
2024-02-09	[posen.com]	abyss	<a href="#">Link</a>
2024-02-09	[macqueeneq.com]	lockbit3	<a href="#">Link</a>
2024-02-09	[parksite.com]	cactus	<a href="#">Link</a>
2024-02-07	[galbusera.it]	lockbit3	<a href="#">Link</a>
2024-02-08	[Ducont]	hunters	<a href="#">Link</a>
2024-02-08	[perkinsmfg.com]	lockbit3	<a href="#">Link</a>
2024-02-08	[originalfootwear.com]	lockbit3	<a href="#">Link</a>
2024-02-08	[Jewish Home Lifecare]	alphv	<a href="#">Link</a>
2024-02-08	[Distecna]	akira	<a href="#">Link</a>
2024-02-07	[Western Municipal Construction]	blacksuit	<a href="#">Link</a>
2024-02-07	[Southwest Binding & Laminating]	blacksuit	<a href="#">Link</a>
2024-02-07	[TeraGo]	akira	<a href="#">Link</a>
2024-02-07	[transaxle.com]	abyss	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-07	[Anderco PTE LTD]	8base	<a href="#">Link</a>
2024-02-07	[Tetrosyl Group Limited]	8base	<a href="#">Link</a>
2024-02-07	[Therme Laa Hotel and Silent Spa]	8base	<a href="#">Link</a>
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	<a href="#">Link</a>
2024-02-07	[YRW Limited - Chartered Accountants]	8base	<a href="#">Link</a>
2024-02-06	[axsbolivia.com]	lockbit3	<a href="#">Link</a>
2024-02-06	[vimarequipment.com]	lockbit3	<a href="#">Link</a>
2024-02-06	[deltron.com]	abyss	<a href="#">Link</a>
2024-02-06	[B&B Electric Inc]	bianlian	<a href="#">Link</a>
2024-02-06	[AVer Information]	akira	<a href="#">Link</a>
2024-02-06	[Celeste]	akira	<a href="#">Link</a>
2024-02-06	[ArpuPlus]	medusa	<a href="#">Link</a>
2024-02-06	[gocco.com]	cactus	<a href="#">Link</a>
2024-02-06	[spbglobal.com]	cactus	<a href="#">Link</a>
2024-02-05	[Modern Kitchens]	play	<a href="#">Link</a>
2024-02-05	[Greenwich Leisure]	play	<a href="#">Link</a>
2024-02-05	[Ready Mixed Concrete]	play	<a href="#">Link</a>
2024-02-05	[Northeastern Sheet Metal]	play	<a href="#">Link</a>
2024-02-05	[Hannon Transport]	play	<a href="#">Link</a>
2024-02-05	[McMillan Pazdan Smith]	play	<a href="#">Link</a>
2024-02-05	[Mason Construction]	play	<a href="#">Link</a>
2024-02-05	[Albert Bartlett]	play	<a href="#">Link</a>
2024-02-05	[Perry-McCall Construction]	play	<a href="#">Link</a>
2024-02-05	[Virgin Islands Lottery]	play	<a href="#">Link</a>
2024-02-05	[Premier Facility Management]	play	<a href="#">Link</a>
2024-02-05	[Douglas County Libraries]	play	<a href="#">Link</a>
2024-02-05	[Leaders Staffing]	play	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-06	[asecos.com]	blackbasta	<a href="#">Link</a>
2024-02-05	[GRUPO SCA[Release of all data]]	knight	<a href="#">Link</a>
2024-02-05	[themisbourne.co.uk]	lockbit3	<a href="#">Link</a>
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	<a href="#">Link</a>
2024-02-05	[hutchpaving.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[davis-french-associates.co.uk]	lockbit3	<a href="#">Link</a>
2024-02-05	[Campaign for Tobacco-Free Kids]	blacksuit	<a href="#">Link</a>
2024-02-05	[VCS Observation]	akira	<a href="#">Link</a>
2024-02-05	[noe.wifi.at]	lockbit3	<a href="#">Link</a>
2024-02-05	[ksa-architecture.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[GRTC Transit System]	bianlian	<a href="#">Link</a>
2024-02-05	[semesco.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[ultraflexx.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[tgestiona.br]	lockbit3	<a href="#">Link</a>
2024-02-05	[philogen.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[prima.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[logtainer.com]	lockbit3	<a href="#">Link</a>
2024-02-05	[portline.pt]	lockbit3	<a href="#">Link</a>
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	<a href="#">Link</a>
2024-02-04	[cxm.com]	lockbit3	<a href="#">Link</a>
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	<a href="#">Link</a>
2024-02-04	[Commonwealth Sign]	qilin	<a href="#">Link</a>
2024-02-04	[FEPCO Zona Franca SAS]	knight	<a href="#">Link</a>
2024-02-03	[pbwtulsa.com]	lockbit3	<a href="#">Link</a>
2024-02-02	[Digitel Venezuela]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	<a href="#">Link</a>
2024-02-02	[manitou-group.com]	lockbit3	<a href="#">Link</a>
2024-02-02	[AbelSantosyAsociados]	knight	<a href="#">Link</a>
2024-02-02	[lexcaribbean.com]	lockbit3	<a href="#">Link</a>
2024-02-02	[Law Office of Michael H Joseph]	bianlian	<a href="#">Link</a>
2024-02-02	[Tandem]	bianlian	<a href="#">Link</a>
2024-02-02	[Innovex Downhole Solutions]	play	<a href="#">Link</a>
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	<a href="#">Link</a>
2024-02-01	[DIROX LTDA (Vietnã)]	knight	<a href="#">Link</a>
2024-02-01	[etsolutions.com.mx]	threeam	<a href="#">Link</a>
2024-02-01	[gatesshields.com]	lockbit3	<a href="#">Link</a>
2024-02-01	[manchesterfertility.com]	lockbit3	<a href="#">Link</a>
2024-02-01	[stemcor.com]	lockbit3	<a href="#">Link</a>
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	<a href="#">Link</a>
2024-02-01	[dms-imaging]	cuba	<a href="#">Link</a>
2024-02-01	[bandcllp.com]	lockbit3	<a href="#">Link</a>
2024-02-01	[taloninternational.com]	lockbit3	<a href="#">Link</a>
2024-02-01	[Southwark Council]	meow	<a href="#">Link</a>
2024-02-01	[Robert D. Clements Jr Law Group, LLLP]	bianlian	<a href="#">Link</a>
2024-02-01	[CNPC Peru S.A.]	rhysida	<a href="#">Link</a>
2024-02-01	[Primeimaging database for sale]	everest	<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.