

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240122



## 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) . . . . .	5
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	8
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>11</b>
4.1 Exploits der letzten 5 Tage . . . . .	11
4.2 0-Days der letzten 5 Tage . . . . .	15
<b>5 Die Hacks der Woche</b>	<b>16</b>
5.0.1 WILDE GitLab Lücke (jeden Account übernehmen) & Probleme mit dem AI Hype	16
<b>6 Cyberangriffe: (Jan)</b>	<b>17</b>
<b>7 Ransomware-Erpressungen: (Jan)</b>	<b>17</b>
<b>8 Quellen</b>	<b>23</b>
8.1 Quellenverzeichnis . . . . .	23
<b>9 Impressum</b>	<b>25</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

#### ***Kritische VMware-Sicherheitslücke wird angegriffen***

Ende Oktober hat VMware ein Update gegen eine kritische Sicherheitslücke herausgegeben. Inzwischen wird das Leck angegriffen.

- [Link](#)

—

#### ***Angriffe attackieren Ivanti EPMM und MobileIron Core***

Angriffe nutzen derzeit eine kritische Sicherheitslücke in Ivanti EPMM und MobileIron Core aus.

- [Link](#)

—

#### ***Nextcloud: Lücken in Apps gefährden Nutzerkonten und Datensicherheit***

In mehreren Erweiterungen, etwa zur Lastverteilung, zur Anmeldung per OAuth und ZIP-Download, klaffen Löcher. Updates sind bereits verfügbar.

- [Link](#)

—

#### ***Trend Micro: Sicherheitslücken in Security-Agents ermöglichen Rechteausweitung***

Trend Micro warnt vor Sicherheitslücken in den Security-Agents, durch die Angreifer ihre Rechte ausweiten können. Software-Updates stehen bereit.

- [Link](#)

—

#### ***MOVEit Transfer: Updates gegen DOS-Lücke***

Updates für MOVEit Transfer dichten Sicherheitslecks ab, durch die Angreifer Rechenfehler provozieren oder den Dienst lahmlegen können.

- [Link](#)

—

#### ***Critical Patch Update: Oracle veröffentlicht 389 Sicherheitsupdates***

Oracle hat in seinem Quartalsupdate unter anderem Banking Enterprise, MySQL und Solaris gegen mögliche Angriffe abgesichert.

- [Link](#)

—

#### ***Jetzt patchen! Vorsicht vor DoS-Angriffen auf Citrix NetScaler ADC und Gateway***

Citrix hat Produkte seiner NetScaler-Serie auf den aktuellen Stand gebracht und gegen laufende Attacken gerüstet.

- [Link](#)

—

**Google Chrome: Sicherheitslücke wird in freier Wildbahn ausgenutzt**

Google aktualisiert den Webbrowser Chrome. Das Update schließt hochriskante Sicherheitslücken. Eine davon wird bereits missbraucht.

- [Link](#)

---

**Kritische Sicherheitslücke: VMware vergaß Zugriffskontrollen in Aria Automation**

Angreifer mit einem gültigen Konto können sich erweiterte Rechte verschaffen. VMware bietet Patches an, Cloud-Kunden bleiben verschont.

- [Link](#)

---

**Atlassian: Updates zum Patchday schließen 28 hochriskante Schwachstellen**

Atlassian veranstaltet einen Patchday und schließt dabei 28 Sicherheitslücken in diversen Programmen, die als hohes Risiko gelten.

- [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	Link	Beschreibung
-----	------	-----------	------	--------------

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

Mon, 22 Jan 2024

**[NEU] [hoch] Lexmark Laser Printers: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Lexmark Laser Printers und Lexmark Multifunction Printer ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 19 Jan 2024

**[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 19 Jan 2024

**[NEU] [hoch] IBM App Connect Enterprise: Schwachstelle ermöglicht Denial of Service oder Offenlegung von Informationen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM App Connect Enterprise ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Fri, 19 Jan 2024

**[NEU] [UNGEPATCHT] [hoch] Internet Browser: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen Internet Browsern, wie z.B. Mozilla Firefox ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 19 Jan 2024

**[UPDATE] [kritisch] Node.js: Mehrere Schwachstellen**

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 19 Jan 2024

**[NEU] [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](#)

—

Fri, 19 Jan 2024

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of

Service Angriff und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 19 Jan 2024

**[UPDATE] [hoch] Apple iOS: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, vertrauliche Kernel-Zustände zu verändern, seine Privilegien zu erhöhen, einen Denial-of-Service zu verursachen oder Sicherheitsmaßnahmen zu umgehen. Eine erfolgreiche Ausnutzung erfordert eine Benutzer-interaktion.

- [Link](#)

—

Fri, 19 Jan 2024

**[UPDATE] [kritisch] Ivanti Endpoint Manager Mobile.: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ivanti Endpoint Manager Mobile. ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programm-code auszuführen.

- [Link](#)

—

Fri, 19 Jan 2024



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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 19 Jan 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](#)

—

Fri, 19 Jan 2024

**[UPDATE] [kritisch] VMware vCenter Server: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in VMware vCenter Server ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 19 Jan 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Fri, 19 Jan 2024

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

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

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
1/19/2024	[Oracle MySQL Enterprise Monitor (January 2024 CPU)]	critical
1/19/2024	[VMware Aria Automation Access Control Vulnerability (VMSA-2024-0001)]	critical
1/19/2024	[Mitsubishi MELSEC-F Series Insufficient Verification of Data Authenticity (CVE-2023-4699)]	critical
1/21/2024	[Fedora 38 : dotnet6.0 (2024-60bc18acfb)]	high
1/21/2024	[Slackware Linux 15.0 / current tigervnc Multiple Vulnerabilities (SSA:2024-021-01)]	high
1/21/2024	[Debian dla-3713 : libcppunit-subunit-dev - security update]	high
1/21/2024	[Fedora 39 : tigervnc / xorg-x11-server (2024-5762d637dd)]	high
1/21/2024	[Fedora 39 : xorg-x11-server (2024-2815d55cdf)]	high
1/21/2024	[RHEL 9 : openssl (RHSA-2024:0310)]	high
1/20/2024	[openSUSE 15 Security Update : chromium (openSUSE-SU-2024:0025-1)]	high
1/20/2024	[Oracle Linux 8 : java-21-openjdk (ELSA-2024-0248)]	high
1/20/2024	[Oracle Linux 9 : java-21-openjdk (ELSA-2024-0249)]	high
1/20/2024	[FreeBSD : electron26 – Out of bounds memory access in V8 (2264566a-a890-46eb-a895-7881dd220bd0)]	high
1/20/2024	[SUSE SLED15 Security Update : xwayland (SUSE-SU-2024:0165-1)]	high
1/20/2024	[Rockwell FactoryTalk Services Platform 2.74 Authentication Bypass]	high
1/20/2024	[AlmaLinux 9 : java-17-openjdk (ALSA-2024:0267)]	high
1/20/2024	[AlmaLinux 9 : java-1.8.0-openjdk (ALSA-2024:0265)]	high
1/20/2024	[AlmaLinux 9 : java-21-openjdk (ALSA-2024:0249)]	high
1/20/2024	[AlmaLinux 9 : java-11-openjdk (ALSA-2024:0266)]	high
1/20/2024	[AlmaLinux 8 : java-21-openjdk (ALSA-2024:0248)]	high
1/20/2024	[Fedora 39 : dotnet6.0 (2024-da73f3fc92)]	high

Datum	Schwachstelle	Bewertung
1/19/2024	[Oracle MySQL Connectors C++ and ODBC (January 2024 CPU)]	high
1/19/2024	[Qnap VioStor < 5.0.0 Command Injection (CVE-2023-47565)]	high
1/19/2024	[Qnap VioStor < 5.0.0 Command Injection (CVE-2023-47565)]	high
1/19/2024	[SUSE SLES12 Security Update : rear27a (SUSE-SU-2024:0135-1)]	high
1/19/2024	[SUSE SLES12 Security Update : rear23a (SUSE-SU-2024:0148-1)]	high
1/19/2024	[Drupal < 9.5.11 / 10.0 DoS]	high
1/19/2024	[Oracle MySQL Server 8.x < 8.3.0 (January 2024 CPU)]	high
1/19/2024	[Oracle MySQL Server 8.0.x < 8.0.36 (January 2024 CPU)]	high
1/19/2024	[JetBrains IntelliJ IDEA < 2023.2 Execution with Unnecessary Privileges (macOS)]	high
1/19/2024	[Oracle MySQL Workbench < 8.0.36 (January 2024)]	high
1/19/2024	[Atlassian Confluence < 7.19.17 / 8.0.x < 8.5.5 / 8.6.x < 8.7.2 (CONFSERVER-93516)]	high
1/19/2024	[Oracle Enterprise Manager Ops Center (January 2024 CPU)]	high
1/19/2024	[Oracle Enterprise Manager Cloud Control (January 2024 CPU)]	high
1/19/2024	[Oracle JDeveloper Multiple Vulnerabilities (January 2024 CPU)]	high
1/19/2024	[Amazon Corretto Java 8.x < 8.402.08.1 Vulnerability]	high
1/19/2024	[Fedora 38 : sos (2024-2fb8991c68)]	high
1/19/2024	[Fedora 39 : sos (2024-a2129a4eb5)]	high
1/19/2024	[Fedora 39 : golang (2024-193547def8)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Fri, 19 Jan 2024

#### **Apache Commons Text 1.9 Remote Code Execution**

This Metasploit module exploit takes advantage of the StringSubstitutor interpolator class, which is included in the Commons Text library. A default interpolator allows for string lookups that can lead to remote code execution. This is due to a logic flaw that makes the script, dns and url lookup keys interpolated by default, as opposed to what it should be, according to the documentation of the StringLookupFactory class. Those keys allow an attacker to execute arbitrary code via lookups primarily using the script key. In order to exploit the vulnerabilities, the following requirements must be met: Run a version of Apache Commons Text from version 1.5 to 1.9, use the StringSubstitutor interpolator, and the target should run JDK versions prior to 15.

- [Link](#)

—

” “Fri, 19 Jan 2024

#### **Linux 5.6 io\_uring Cred Refcount Overflow**

Linux versions 5.6 and above appear to suffer from a cred refcount overflow when handling approximately 39 gigabytes of memory usage via io\_uring.

- [Link](#)

—

” “Fri, 19 Jan 2024

#### **Lepton CMS 7.0.0 Remote Code Execution**

Lepton CMS version 7.0.0 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Fri, 19 Jan 2024

#### **Firefox 121 / Chrome 120 Denial Of Service**

Firefox version 121 and Chrome version 120 may both suffer from a minor denial of service issue with file downloads.

- [Link](#)

—

” “Fri, 19 Jan 2024

#### **MiniWeb HTTP Server 0.8.1 Denial Of Service**

MiniWeb HTTP Server version 0.8.1 remote denial of service exploit.

- [Link](#)

—

” “Thu, 18 Jan 2024

### **WordPress Backup Migration 1.3.7 Remote Command Execution**

This Metasploit module exploits an unauthenticated remote command execution vulnerability in WordPress Backup Migration plugin versions 1.3.7 and below. The vulnerability is exploitable through the Content-Dir header which is sent to the /wp-content/plugins/backup-backup/includes/backup-heart.php endpoint. The exploit makes use of a neat technique called PHP Filter Chaining which allows an attacker to prepend bytes to a string by continuously chaining character encoding conversions. This allows an attacker to prepend a PHP payload to a string which gets evaluated by a require statement, which results in command execution.

- [Link](#)

—

” “Thu, 18 Jan 2024

### **Ansible Agent Payload Deployer**

This exploit module creates an ansible module for deployment to nodes in the network. It creates a new yaml playbook which copies our payload, chmods it, then runs it on all targets which have been selected (default all).

- [Link](#)

—

” “Thu, 18 Jan 2024

### **SpyCamLizard 1.230 Denial Of Service**

SpyCamLizard version 1.230 remote denial of service exploit.

- [Link](#)

—

” “Thu, 18 Jan 2024

### **Legends Of IdleOn Random Number Generation Manipulation**

Legends of IdleOn suffers from use of an insecure random number generator that can be replaced by a malicious user.

- [Link](#)

—

” “Wed, 17 Jan 2024

### **Easy File Sharing FTP 3.6 Denial Of Service**

Easy File Sharing FTP version 3.6 remote denial of service exploit.

- [Link](#)

—

” “Wed, 17 Jan 2024

### **PixieFail Proof Of Concepts**

This archive contains proof of concepts to trigger the 7 vulnerabilities in Tianocore’s EDK II open source implementation of the UEFI specification. Issues include an integer underflow, buffer over-

flows, infinite loops, and an out of bounds read.

- [Link](#)

—

” “Tue, 16 Jan 2024

***MailCarrier 2.51 Denial Of Service***

MailCarrier version 2.51 remote denial of service exploit.

- [Link](#)

—

” “Tue, 16 Jan 2024

***LightFTP 1.1 Denial Of Service***

LightFTP version 1.1 remote denial of service exploit.

- [Link](#)

—

” “Mon, 15 Jan 2024

***Korenix JetNet Series Unauthenticated Access***

Korenix JetNet Series allows TFTP without authentication and also allows for unauthenticated firmware upgrades.

- [Link](#)

—

” “Mon, 15 Jan 2024

***WordPress RSVPMaker 9.3.2 SQL Injection***

WordPress RSVPMaker plugin versions 9.3.2 and below suffer from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 15 Jan 2024

***Taokeyun SQL Injection***

Taokeyun versions up to 1.0.5 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 15 Jan 2024

***HaoKeKeJi YiQiNiu Server-Side Request Forgery***

HaoKeKeJi YiQiNiu versions up to 3.1 suffer from a server-side request forgery vulnerability.

- [Link](#)

—

” “Mon, 15 Jan 2024

***Xitami 2.5 Denial Of Service***

Xitami version 2.5 remote denial of service exploit.

- [Link](#)

—

” “Sun, 14 Jan 2024

**freeSSHD 1.0.9 Denial Of Service**

freeSSHD version 1.0.9 remote denial of service exploit.

- [Link](#)

—

” “Sat, 13 Jan 2024

**ProSSHD 1.2 20090726 Denial Of Service**

ProSSHD version 1.2 20090726 remote denial of service exploit.

- [Link](#)

—

” “Fri, 12 Jan 2024

**macOS AppleVADriver Out-Of-Bounds Write**

macOS suffers from an out-of-bounds write vulnerability in AppleVADriver when decoding mpeg2 videos.

- [Link](#)

—

” “Fri, 12 Jan 2024

**macOS AppleGVA Memory Handling**

On Intel macOS, HEVC video decoding is performed in the AppleGVA module. Using fuzzing, researchers identified multiple issues in this decoder. The issues range from out-of-bounds writes, out-of-bounds reads and, in one case, free() on an invalid address. All of the issues were reproduced on macOS Ventura 13.6 running on a 2018 Mac mini (Intel based).

- [Link](#)

—

” “Fri, 12 Jan 2024

**Linux 4.20 KTLS Read-Only Write**

Linux versions 4.20 and above have an issue where ktls writes into spliced readonly pages.

- [Link](#)

—

” “Fri, 12 Jan 2024

**Linux Broken Unix GC Interaction Use-After-Free**

Linux suffers from an io\_uring use-after-free vulnerability due to broken unix GC interaction.

- [Link](#)

—

” “Fri, 12 Jan 2024

**Quick TFTP Server Pro 2.1 Denial Of Service**

Quick TFTP Server Pro version 2.1 remote denial of service exploit.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Fri, 19 Jan 2024

**ZDI-24-080: Trend Micro Mobile Security for Enterprises vpplist\_assign\_list Cross-Site Scripting Vulnerability**

- [Link](#)

—

” “Fri, 19 Jan 2024

**ZDI-24-079: Trend Micro Mobile Security for Enterprises ServerUpdate\_UpdateSuccessful Cross-Site Scripting Vulnerability**

- [Link](#)

—

” “Fri, 19 Jan 2024

**ZDI-24-078: Trend Micro Mobile Security for Enterprises DevicesManagementEditNotePopupTip Cross-Site Scripting Vulnerability**

- [Link](#)

—

” “Fri, 19 Jan 2024

**ZDI-24-077: Trend Micro Apex Central Unrestricted File Upload Vulnerability**

- [Link](#)

—

” “Fri, 19 Jan 2024

**ZDI-24-076: Trend Micro Deep Security Link Following Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Fri, 19 Jan 2024

**ZDI-24-075: Trend Micro Deep Security Improper Access Control Local Privilege Escalation Vulnerability**

- [Link](#)

—

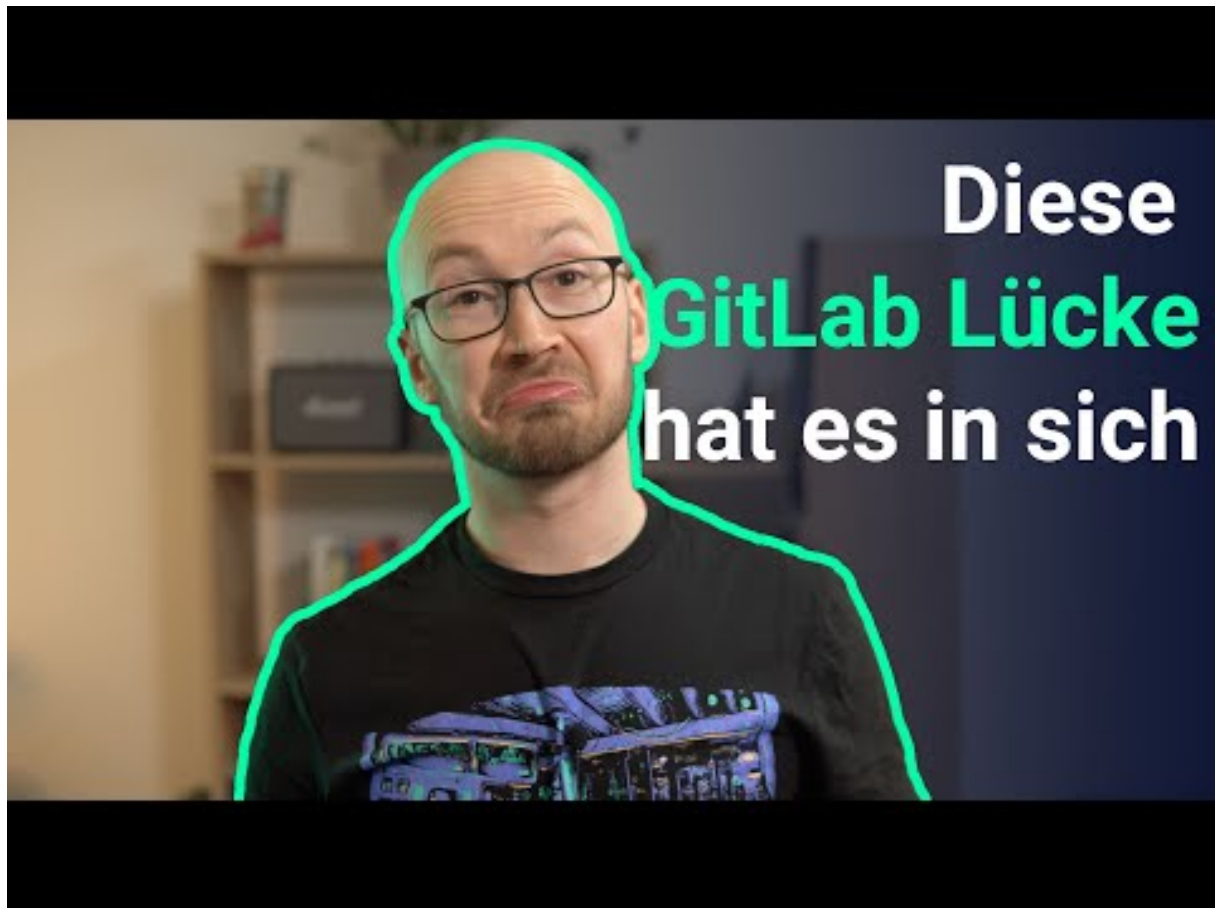
”



## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 WILDE GitLab Lücke (jeden Account übernehmen) & Probleme mit dem AI Hype



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-17	Donau 3 FM	[DEU]	<a href="#">Link</a>
2024-01-17	Service de secours de Jämtland	[SWE]	<a href="#">Link</a>
2024-01-16	Université d'État du Kansas (K-State)	[USA]	<a href="#">Link</a>
2024-01-15	Foxsemicon Integrated Technology Inc (꠆꠆꠆꠆)	[TWN]	<a href="#">Link</a>
2024-01-15	Canterbury City Council, Thanet District Council, Dover District Council.	[GBR]	<a href="#">Link</a>
2024-01-13	Calvia	[ESP]	<a href="#">Link</a>
2024-01-13	Sambr'Habitat	[BEL]	<a href="#">Link</a>
2024-01-10	RE&S Holdings	[JPN]	<a href="#">Link</a>
2024-01-10	Lush	[GBR]	<a href="#">Link</a>
2024-01-06	loanDepot	[USA]	<a href="#">Link</a>
2024-01-06	Banque nationale d'Angola	[AGO]	<a href="#">Link</a>
2024-01-05	Toronto Zoo	[CAN]	<a href="#">Link</a>
2024-01-05	ODAV AG	[DEU]	<a href="#">Link</a>
2024-01-04	City of Beckley	[USA]	<a href="#">Link</a>
2024-01-04	Tigo Business	[PRY]	<a href="#">Link</a>
2024-01-01	Commune de Saint-Philippe	[FRA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Jan)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-21	[synnex-grp.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[gattoplaters.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[duconind.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-21	[wittmann.at]	lockbit3	<a href="#">Link</a>
2024-01-21	[qtc-energy.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[hughessupplyco.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[umi-tiles.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[cct.or.th]	lockbit3	<a href="#">Link</a>
2024-01-22	[cmmt.com.tw]	lockbit3	<a href="#">Link</a>
2024-01-21	[shenandoahtx.us]	lockbit3	<a href="#">Link</a>
2024-01-21	[stjohnrochester.org]	lockbit3	<a href="#">Link</a>
2024-01-21	[bmc-cpa.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[jasman.com.mx]	lockbit3	<a href="#">Link</a>
2024-01-21	[North Star Tax And Accounting]	bianlian	<a href="#">Link</a>
2024-01-21	[KC Pharmaceuticals]	bianlian	<a href="#">Link</a>
2024-01-21	[Martinaire Aviation]	bianlian	<a href="#">Link</a>
2024-01-21	[subway.com]	lockbit3	<a href="#">Link</a>
2024-01-21	[tvjahrheine.de]	lockbit3	<a href="#">Link</a>
2024-01-21	[marxan.es]	lockbit3	<a href="#">Link</a>
2024-01-21	[home-waremmien.be]	lockbit3	<a href="#">Link</a>
2024-01-20	[wendy.mx]	lockbit3	<a href="#">Link</a>
2024-01-20	[swiftair.com]	lockbit3	<a href="#">Link</a>
2024-01-20	[Worthen Industries [You have three days]]	alphv	<a href="#">Link</a>
2024-01-19	[Anna Jaques Hospital]	moneymessage	<a href="#">Link</a>
2024-01-19	[pratt.edu]	lockbit3	<a href="#">Link</a>
2024-01-19	[seiu1000.org]	lockbit3	<a href="#">Link</a>
2024-01-19	[Sykes Consulting, Inc.]	incransom	<a href="#">Link</a>
2024-01-19	[dywidag.com]	lockbit3	<a href="#">Link</a>
2024-01-19	[TPG Architecture]	play	<a href="#">Link</a>
2024-01-12	[jdbchina.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-19	[Hamilton-Madison House]	akira	<a href="#">Link</a>
2024-01-19	[Hydratek]	akira	<a href="#">Link</a>
2024-01-19	[Busse & Busee, PC Attorneys at Law]	alphv	<a href="#">Link</a>
2024-01-19	[evit.edu]	lockbit3	<a href="#">Link</a>
2024-01-19	[Alupar Investimento SA]	hunters	<a href="#">Link</a>
2024-01-19	[PROJECTSW]	qilin	<a href="#">Link</a>
2024-01-19	[foxsemicon.com]	lockbit3	<a href="#">Link</a>
2024-01-09	[Malongo France]	8base	<a href="#">Link</a>
2024-01-18	[Samuel Sekuritas Indonesia & Samuel Aset Manajemen]	trigona	<a href="#">Link</a>
2024-01-18	[Premier Facility Management]	trigona	<a href="#">Link</a>
2024-01-18	[Fertility North]	trigona	<a href="#">Link</a>
2024-01-18	[Vision Plast]	trigona	<a href="#">Link</a>
2024-01-18	[uffs.edu.br]	stormous	<a href="#">Link</a>
2024-01-18	[Groveport Madison Schools]	blacksuit	<a href="#">Link</a>
2024-01-18	[GROWTH by NCRC]	bianlian	<a href="#">Link</a>
2024-01-18	[LT Business Dynamics]	bianlian	<a href="#">Link</a>
2024-01-18	[digipwr.com]	lockbit3	<a href="#">Link</a>
2024-01-18	[jaffeandasher.com]	lockbit3	<a href="#">Link</a>
2024-01-18	[Gallup McKinley County Schools]	hunters	<a href="#">Link</a>
2024-01-15	[aercap.com]	slug	<a href="#">Link</a>
2024-01-17	[DENHAM the Jeanmaker]	akira	<a href="#">Link</a>
2024-01-17	[Stone, Avant & Daniels]	medusa	<a href="#">Link</a>
2024-01-17	[JspPharma]	insane	<a href="#">Link</a>
2024-01-16	[Axfast AB]	8base	<a href="#">Link</a>
2024-01-16	[Syndicat Général des Vignerons de la Champagne]	8base	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-16	[Washtech]	8base	<a href="#">Link</a>
2024-01-16	[SIVAM Coatings S.p.A.]	8base	<a href="#">Link</a>
2024-01-16	[Nexus Telecom Switzerland AG]	8base	<a href="#">Link</a>
2024-01-16	[millgate.co.uk]	lockbit3	<a href="#">Link</a>
2024-01-16	[Becker Logistics]	akira	<a href="#">Link</a>
2024-01-16	[Bestway Sales]	akira	<a href="#">Link</a>
2024-01-16	[TGS Transportation]	akira	<a href="#">Link</a>
2024-01-16	[Premium Guard]	akira	<a href="#">Link</a>
2024-01-16	[F J O'Hara & Sons]	qilin	<a href="#">Link</a>
2024-01-16	[Donear Industries]	bianlian	<a href="#">Link</a>
2024-01-15	[Beit Handesai]	malekteam	<a href="#">Link</a>
2024-01-15	[shinwajpn.co.jp]	lockbit3	<a href="#">Link</a>
2024-01-15	[maisonsdelavenir.com]	lockbit3	<a href="#">Link</a>
2024-01-15	[vasudhapharma.com]	lockbit3	<a href="#">Link</a>
2024-01-15	[hosted-it.co.uk]	lockbit3	<a href="#">Link</a>
2024-01-15	[Ausa]	hunters	<a href="#">Link</a>
2024-01-15	[Republic Shipping Consolidators, Inc]	bianlian	<a href="#">Link</a>
2024-01-15	[Northeast Spine and Sports Medicine's]	bianlian	<a href="#">Link</a>
2024-01-14	[SPARTAN Light Metal Products]	unsafe	<a href="#">Link</a>
2024-01-14	[Hartl European Transport Company]	unsafe	<a href="#">Link</a>
2024-01-14	[American International College]	unsafe	<a href="#">Link</a>
2024-01-14	[www.kai.id "FF"]	stormous	<a href="#">Link</a>
2024-01-14	[amenitek.com]	lockbit3	<a href="#">Link</a>
2024-01-08	[turascanadinavia.com]	lockbit3	<a href="#">Link</a>
2024-01-13	[Lee Spring]	rhysida	<a href="#">Link</a>
2024-01-11	[Charm Sciences]	snatch	<a href="#">Link</a>
2024-01-11	[Malabar Gold & Diamonds]	snatch	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-11	[Banco Promerica]	snatch	<a href="#">Link</a>
2024-01-12	[arrowinternational.com]	lockbit3	<a href="#">Link</a>
2024-01-12	[thecsi.com]	threeam	<a href="#">Link</a>
2024-01-12	[pharrusa.com]	threeam	<a href="#">Link</a>
2024-01-12	[Builcore]	alphv	<a href="#">Link</a>
2024-01-12	[hotelcontinental.no]	qilin	<a href="#">Link</a>
2024-01-12	[olea.com]	lockbit3	<a href="#">Link</a>
2024-01-12	[asburyauto.com]	cactus	<a href="#">Link</a>
2024-01-12	[Washington School For The Deaf]	incransom	<a href="#">Link</a>
2024-01-12	[Former S.p.A.]	8base	<a href="#">Link</a>
2024-01-12	[International Trade Brokers and Forwarders]	8base	<a href="#">Link</a>
2024-01-12	[BALLAY MENUISERIES]	8base	<a href="#">Link</a>
2024-01-12	[Anderson King Energy Consultants, LLC]	8base	<a href="#">Link</a>
2024-01-12	[Sems and Specials Incorporated]	8base	<a href="#">Link</a>
2024-01-12	[acutis.com]	cactus	<a href="#">Link</a>
2024-01-12	[dtsolutions.net]	cactus	<a href="#">Link</a>
2024-01-12	[intercityinvestments.com]	cactus	<a href="#">Link</a>
2024-01-12	[hi-cone.com]	cactus	<a href="#">Link</a>
2024-01-12	[Alliedwoundcare]	everest	<a href="#">Link</a>
2024-01-12	[Primeimaging]	everest	<a href="#">Link</a>
2024-01-11	[Blackburn College]	akira	<a href="#">Link</a>
2024-01-11	[Vincentz Network]	akira	<a href="#">Link</a>
2024-01-11	[Limburg]	medusa	<a href="#">Link</a>
2024-01-11	[Water For People]	medusa	<a href="#">Link</a>
2024-01-11	[pactchangeslives.com]	lockbit3	<a href="#">Link</a>
2024-01-11	[Triella]	alphv	<a href="#">Link</a>
2024-01-11	[Ursel Phillips Fellows Hopkinson]	alphv	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-11	[SHIBLEY RIGHTON]	alphv	<a href="#">Link</a>
2024-01-11	[automotionsshade.com]	alphv	<a href="#">Link</a>
2024-01-11	[R Robertson Insurance Brokers]	alphv	<a href="#">Link</a>
2024-01-10	[molnar&partner]	qilin	<a href="#">Link</a>
2024-01-10	[hartalega.com.my]	lockbit3	<a href="#">Link</a>
2024-01-10	[agnesb.eu]	lockbit3	<a href="#">Link</a>
2024-01-10	[twf.co.za]	lockbit3	<a href="#">Link</a>
2024-01-10	[tiautoinvestments.co.za]	lockbit3	<a href="#">Link</a>
2024-01-10	[Group Bogart]	alphv	<a href="#">Link</a>
2024-01-09	[Delco Automation]	blacksuit	<a href="#">Link</a>
2024-01-09	[Viridi]	akira	<a href="#">Link</a>
2024-01-09	[Ito Pallpack Gruppen]	akira	<a href="#">Link</a>
2024-01-09	[Corinth Coca-Cola Bottling Works]	qilin	<a href="#">Link</a>
2024-01-09	[Precision Tune Auto Care]	8base	<a href="#">Link</a>
2024-01-08	[Erbilbil Bilgisayar]	alphv	<a href="#">Link</a>
2024-01-08	[HALLEONARD]	qilin	<a href="#">Link</a>
2024-01-08	[Van Buren Public Schools]	akira	<a href="#">Link</a>
2024-01-08	[Heller Industries]	akira	<a href="#">Link</a>
2024-01-08	[CellNetix Pathology & Laboratories, LLC]	incransom	<a href="#">Link</a>
2024-01-08	[mciwv.com]	lockbit3	<a href="#">Link</a>
2024-01-08	[morganpilate.com]	lockbit3	<a href="#">Link</a>
2024-01-07	[capitalhealth.org]	lockbit3	<a href="#">Link</a>
2024-01-07	[Flash-Motors Last Warning]	raznatovic	<a href="#">Link</a>
2024-01-07	[Agro Baggio LTDA]	knight	<a href="#">Link</a>
2024-01-06	[Maas911.com]	cloak	<a href="#">Link</a>
2024-01-06	[GRUPO SCA]	knight	<a href="#">Link</a>
2024-01-06	[Televerde]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-06	[The Lutheran World Federation]	rhysida	<a href="#">Link</a>
2024-01-05	[Proax Technologies LTD]	bianlian	<a href="#">Link</a>
2024-01-05	[Somerset Logistics]	bianlian	<a href="#">Link</a>
2024-01-05	[ips-securex.com]	lockbit3	<a href="#">Link</a>
2024-01-04	[Project M.O.R.E.]	hunters	<a href="#">Link</a>
2024-01-04	[Thermosash Commercial Ltd]	hunters	<a href="#">Link</a>
2024-01-04	[Gunning & LaFazia, Inc.]	hunters	<a href="#">Link</a>
2024-01-04	[Diablo Valley Oncology and Hematology Medical Group - Press Release]	monti	<a href="#">Link</a>
2024-01-03	[Kershaw County School District]	blacksuit	<a href="#">Link</a>
2024-01-03	[Bradford Health]	hunters	<a href="#">Link</a>
2024-01-02	[groupe-idea.com]	lockbit3	<a href="#">Link</a>
2024-01-02	[SAED International]	alphv	<a href="#">Link</a>
2024-01-02	[graebener-group.com]	blackbasta	<a href="#">Link</a>
2024-01-02	[leonardsexpress.com]	blackbasta	<a href="#">Link</a>
2024-01-02	[nals.com]	blackbasta	<a href="#">Link</a>
2024-01-02	[MPM Medical Supply]	ciphbit	<a href="#">Link</a>
2024-01-01	[DELPHINUS.COM]	clop	<a href="#">Link</a>
2024-01-01	[Aspiration Training]	rhysida	<a href="#">Link</a>
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	<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.