

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240106



## 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) . . . . .	6
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	9
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>12</b>
4.1 Exploits der letzten 5 Tage . . . . .	12
4.2 0-Days der letzten 5 Tage . . . . .	16
<b>5 Die Hacks der Woche</b>	<b>18</b>
5.0.1 Ihr habt WAS in eure Züge programmiert!? ☒ . . . . .	19
<b>6 Cyberangriffe: (Jan)</b>	<b>20</b>
<b>7 Ransomware-Erpressungen: (Jan)</b>	<b>20</b>
<b>8 Quellen</b>	<b>21</b>
8.1 Quellenverzeichnis . . . . .	21
<b>9 Impressum</b>	<b>22</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 Schadcode-Lücke gefährdet Ivanti Endpoint Manager***

Unter bestimmten Voraussetzungen können Angreifer Schadcode auf Ivanti-EPM-Servern ausführen.

- [Link](#)

---

#### ***Netzwerkanalysetool Wireshark gegen mögliche Attacken abgesichert***

Die Wireshark-Entwickler haben in aktuellen Versionen mehrere Sicherheitslücken geschlossen.

- [Link](#)

---

#### ***Patchday Android: Angreifer können sich höhere Rechte erschleichen***

Android-Geräte sind für Attacken anfällig. Google, Samsung & Co. stellen Sicherheitsupdates bereit.

- [Link](#)

---

#### ***Update für Google Chrome schließt sechs Sicherheitslücken***

Google hat aktualisierte Chrome-Versionen herausgegeben. Sie schließen sechs Sicherheitslücken, davon mehrere mit hohem Risiko.

- [Link](#)

---

#### ***Lücke in Barracuda E-Mail Security Gateway ermöglichte Code-Einschleusung***

Einfallstor für die Sicherheitslücke ist ein Excel-Parser. Barracuda hat bereits Patches auf allen betroffenen Geräten ausgerollt.

- [Link](#)

---

#### ***Sicherheitsupdate: Schadcode-Attacken auf Juniper Secure Analytics möglich***

Angreifer können Junipers SIEM-System Secure Analytics ins Visier nehmen. Sicherheitspatches sind verfügbar.

- [Link](#)

---

#### ***Kritische Sicherheitslücke in Perl-Bibliothek: Schwachstelle bereits ausgenutzt***

In einer Perl-Bibliothek zum Parsen von Excel-Dateien haben Sicherheitsforscher eine kritische Schwachstelle entdeckt, die Angreifer bereits ausgenutzt haben.

- [Link](#)

---

#### ***Kritische Lücken in Mobile-Device-Management-Lösung Ivanti Avalanche geschlossen***

Angreifer können Ivanti Avalanche mit Schadcode attackieren. Eine reparierte Version steht zum

Download bereit.

- [Link](#)

—

***Google Chrome: Zero-Day-Lücke wird angegriffen, Update verfügbar***

Googles Entwickler haben ein Update für Chrome veröffentlicht, das eine bereits angegriffene Sicherheitslücke abdichtet.

- [Link](#)

—

***Firefox und Thunderbird: Sicherheitslücken geschlossen und Funktionen ergänzt***

Die neuen Versionen von Firefox und Thunderbird dichten Sicherheitslecks ab. Zudem bringen sie neue Funktionen mit.

- [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-2023-5360	0.967230000	0.995790000	<a href="#">Link</a>
CVE-2023-4966	0.917920000	0.987030000	<a href="#">Link</a>
CVE-2023-46747	0.965530000	0.995210000	<a href="#">Link</a>
CVE-2023-46604	0.968050000	0.996100000	<a href="#">Link</a>
CVE-2023-42793	0.972830000	0.998350000	<a href="#">Link</a>
CVE-2023-38035	0.971630000	0.997650000	<a href="#">Link</a>
CVE-2023-35078	0.948640000	0.991090000	<a href="#">Link</a>
CVE-2023-34634	0.906880000	0.985820000	<a href="#">Link</a>
CVE-2023-34039	0.921440000	0.987370000	<a href="#">Link</a>
CVE-2023-33246	0.971220000	0.997470000	<a href="#">Link</a>
CVE-2023-32315	0.964530000	0.994780000	<a href="#">Link</a>
CVE-2023-30625	0.939660000	0.989620000	<a href="#">Link</a>
CVE-2023-30013	0.944370000	0.990360000	<a href="#">Link</a>
CVE-2023-28771	0.923800000	0.987740000	<a href="#">Link</a>
CVE-2023-27524	0.906500000	0.985790000	<a href="#">Link</a>
CVE-2023-27372	0.970430000	0.997000000	<a href="#">Link</a>
CVE-2023-27350	0.972290000	0.998030000	<a href="#">Link</a>
CVE-2023-26469	0.938510000	0.989490000	<a href="#">Link</a>
CVE-2023-26360	0.942270000	0.989960000	<a href="#">Link</a>
CVE-2023-26035	0.968020000	0.996080000	<a href="#">Link</a>
CVE-2023-25717	0.954350000	0.992220000	<a href="#">Link</a>
CVE-2023-25194	0.908370000	0.985970000	<a href="#">Link</a>
CVE-2023-2479	0.958820000	0.993240000	<a href="#">Link</a>
CVE-2023-24489	0.968700000	0.996370000	<a href="#">Link</a>
CVE-2023-22518	0.965250000	0.995070000	<a href="#">Link</a>
CVE-2023-22515	0.955290000	0.992430000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21839	0.962040000	0.994040000	<a href="#">Link</a>
CVE-2023-21823	0.940060000	0.989690000	<a href="#">Link</a>
CVE-2023-21554	0.961220000	0.993770000	<a href="#">Link</a>
CVE-2023-20887	0.961530000	0.993850000	<a href="#">Link</a>
CVE-2023-1671	0.957690000	0.993000000	<a href="#">Link</a>
CVE-2023-0669	0.966690000	0.995560000	<a href="#">Link</a>

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

Fri, 05 Jan 2024

**[NEU] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 05 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 05 Jan 2024

**[NEU] [hoch] NCP Secure Enterprise Client: Schwachstelle ermöglicht Privilegieneskalation und Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in NCP Secure Enterprise Client ausnutzen, um seine Privilegien zu erhöhen und zur Ausführung von beliebigem Code.

- [Link](#)

—

Fri, 05 Jan 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 05 Jan 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](#)

—

Fri, 05 Jan 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](#)

—

Fri, 05 Jan 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](#)

—

Fri, 05 Jan 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](#)

—

Fri, 05 Jan 2024

**[UPDATE] [hoch] SMTP Implementierungen: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen SMTP Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 05 Jan 2024

**[NEU] [hoch] Ivanti Endpoint Manager: Schwachstelle ermöglicht Codeausführung**



Ein Angreifer aus dem lokalen Netzwerk kann eine Schwachstelle in Ivanti Endpoint Manager ausnutzen, um beliebigen Programmcode auszuführen und die Kontrolle über verwaltete Geräte übernehmen.

- [Link](#)

—

Thu, 04 Jan 2024

**[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 04 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](#)

—

Thu, 04 Jan 2024

**[NEU] [hoch] Google Android und Pixel Patchday Januar 2024**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder seine Rechte zu erweitern.

- [Link](#)

—

Wed, 03 Jan 2024

**[UPDATE] [hoch] Apache Struts: Schwachstelle ermöglicht Denial of Service**

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

- [Link](#)

—

Wed, 03 Jan 2024

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

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

- [Link](#)

—

Wed, 03 Jan 2024

**[UPDATE] [kritisch] Apache Struts: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache Struts ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 03 Jan 2024

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

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

- [Link](#)

—

Wed, 03 Jan 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, 03 Jan 2024

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

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

- [Link](#)

—

Wed, 03 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
1/5/2024	[GLSA-202401-04 : WebKitGTK+: Multiple Vulnerabilities]	critical
1/5/2024	[GLSA-202401-02 : c-ares: Multiple Vulnerabilities]	critical
1/4/2024	[Fedora 39 : chromium (2024-210776b8c7)]	critical
1/4/2024	[Festo CECC-X-M1 OS Command Injection (CVE-2022-30309)]	critical
1/4/2024	[Festo CECC-X-M1 OS Command Injection (CVE-2022-30311)]	critical
1/4/2024	[Festo CECX-X-(C1/M1) Improper Authentication (CVE-2014-0760)]	critical
1/4/2024	[Festo CECC-X-M1 OS Command Injection (CVE-2022-30308)]	critical
1/4/2024	[Festo CECC-X-M1 OS Command Injection (CVE-2022-30310)]	critical
1/5/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libcryptopp (SUSE-SU-2024:0030-1)]	high
1/5/2024	[GLSA-202401-06 : CUPS filters: Remote Code Execution]	high
1/5/2024	[GLSA-202401-05 : RDoc: Command Injection]	high
1/5/2024	[Ubuntu 22.04 LTS : Linux kernel (Intel IoTG) vulnerabilities (USN-6549-4)]	high
1/5/2024	[Apache OpenOffice < 4.1.15 Multiple Vulnerabilities (macOS)]	high
1/5/2024	[Apache OpenOffice < 4.1.15 Multiple Vulnerabilities]	high
1/5/2024	[Microsoft Edge (Chromium) < 120.0.2210.121 Multiple Vulnerabilities]	high
1/4/2024	[AlmaLinux 9 : firefox (ALSA-2024:0025)]	high
1/4/2024	[AlmaLinux 9 : tigervnc (ALSA-2024:0010)]	high
1/4/2024	[AlmaLinux 9 : thunderbird (ALSA-2024:0001)]	high
1/4/2024	[Oracle Linux 8 : tigervnc (ELSA-2024-0018)]	high
1/4/2024	[Oracle Linux 8 : squid:4 (ELSA-2024-0046)]	high
1/4/2024	[AlmaLinux 8 : firefox (ALSA-2024:0012)]	high
1/4/2024	[AlmaLinux 8 : tigervnc (ALSA-2024:0018)]	high
1/4/2024	[AlmaLinux 8 : thunderbird (ALSA-2024:0003)]	high
1/4/2024	[AlmaLinux 8 : squid:4 (ALSA-2024:0046)]	high

Datum	Schwachstelle	Bewertung
1/4/2024	[FreeBSD : electron26 – multiple vulnerabilities (0cee4f9c-5efb-4770-b917-f4e4569e8bec)]	high
1/4/2024	[FreeBSD : electron27 – multiple vulnerabilities (d1b20e09-dbdf-432b-83c7-89f0af76324a)]	high
1/4/2024	[FreeBSD : chromium – multiple security fixes (3ee577a9-aad4-11ee-86bb-a8a1599412c6)]	high
1/4/2024	[Siemens SIMATIC S7-400 Buffer Access with Incorrect Length Value (CVE-2022-47375)]	high
1/4/2024	[Siemens SIMATIC S7-400 Uncontrolled Recursion (CVE-2022-47374)]	high
1/4/2024	[Festo CECX-X-(C1/M1) Improper Authentication (CVE-2014-0769)]	high
1/4/2024	[Cisco NX-OS Software VXLAN OAM (NGOAM) Denial of Service (CVE-2021-1587)]	high
1/4/2024	[Siemens SCALANCE Acceptance of Extraneous Untrusted Data With Trusted Data (CVE-2023-44317)]	high
1/4/2024	[Siemens SCALANCE Unsynchronized Access to Shared Data in a Multithreaded Context (CVE-2023-44374)]	high
1/3/2024	[Wireshark 4.0.x < 4.0.12 Multiple Vulnerabilities]	high
1/3/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : SQLite vulnerabilities (USN-6566-1)]	high
1/3/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6565-1)]	high
1/3/2024	[Oracle Linux 8 : firefox (ELSA-2024-0012)]	high
1/3/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-0003)]	high
1/3/2024	[Wireshark 4.2.x < 4.2.1 Multiple Vulnerabilities]	high
1/3/2024	[Wireshark 4.2.x < 4.2.1 Multiple Vulnerabilities (macOS)]	high
1/3/2024	[RHEL 8 : squid:4 (RHSA-2024:0046)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Fri, 05 Jan 2024

#### ***Themebleed Windows 11 Themes Arbitrary Code Execution***

When an unpatched Windows 11 host loads a theme file referencing an msstyles file, Windows loads the msstyles file, and if that file's PACKME\_VERSION is 999, it then attempts to load an accompanying dll file ending in \_vrf.dll. Before loading that file, it verifies that the file is signed. It does this by opening the file for reading and verifying the signature before opening the file for execution. Because this action is performed in two discrete operations, it opens the procedure for a time of check to time of use vulnerability. By embedding a UNC file path to an SMB server we control, the SMB server can serve a legitimate, signed dll when queried for the read, but then serve a different file of the same name when the host intends to load/execute the dll.

- [Link](#)

—

” “Fri, 05 Jan 2024

#### ***Easy Chat Server 3.1 Denial Of Service***

Easy Chat Server version 3.1 suffers from a denial of service vulnerability.

- [Link](#)

—

” “Thu, 04 Jan 2024

#### ***Easy File Sharing FTP Server 2.0 Denial Of Service***

Easy File Sharing FTP Server version 2.0 suffers from a denial of service vulnerability.

- [Link](#)

—

” “Wed, 03 Jan 2024

#### ***minaliC 2.0.0 Denial Of Service***

minaliC version 2.0.0 suffers from a denial of service vulnerability.

- [Link](#)

—

” “Wed, 03 Jan 2024

#### ***Microsoft Windows Kernel Information Disclosure***

Any unprivileged, local user in Microsoft Windows can disclose whether a specific file, directory or registry key exists in the system or not, even if they do not have the open right to it or enumerate right to its parent.

- [Link](#)

—

” “Wed, 03 Jan 2024

***Chrome BindTextSuggestionHostForFrame Type Confusion***

Chrome suffers from a type confusion vulnerability in BindTextSuggestionHostForFrame.

- [Link](#)

—

” “Wed, 03 Jan 2024

***WebCalendar 1.3.0 Cross Site Scripting***

WebCalendar version 1.3.0 suffers from reflective and persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Wed, 03 Jan 2024

***CMSMS 2.2.19 Arbitrary File Upload***

CMSMS version 2.2.19 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

” “Tue, 02 Jan 2024

***Packet Storm New Exploits For 2023***

Complete comprehensive archive of all 1,863 exploits added to Packet Storm in 2023.

- [Link](#)

—

” “Tue, 02 Jan 2024

***Packet Storm New Exploits For December, 2023***

This archive contains all of the 74 exploits added to Packet Storm in December, 2023.

- [Link](#)

—

” “Tue, 02 Jan 2024

***Apache 2.4.55 mod\_proxy HTTP Request Smuggling***

Some mod\_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow for an HTTP request smuggling attack. Configurations are affected when mod\_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

- [Link](#)

—

” “Tue, 02 Jan 2024

***FTPDMIN 0.96 Denial Of Service***

FTPDMIN version 0.96 suffers from a denial of service vulnerability.

- [Link](#)

—  
" "Tue, 02 Jan 2024

***Ultra Mini HTTPd 1.21 Denial Of Service***

Ultra Mini HTTPd version 1.21 suffers from a denial of service vulnerability.

- [Link](#)

—

" "Fri, 29 Dec 2023

***Apache OFBiz 18.12.09 Remote Code Execution***

Apache OFBiz version 18.12.09 suffers from a pre-authentication remote code execution vulnerability.

- [Link](#)

—

" "Thu, 28 Dec 2023

***Microsoft Windows PowerShell Code Execution / Event Log Bypass***

Prior work from this researcher disclosed how PowerShell executes unintended files or BASE64 code when processing specially crafted filenames. This research builds on their PSTrojanFile work, adding a PS command line single quote bypass and PS event logging failure. On Windows CL tab, completing a filename uses double quotes that can be leveraged to trigger arbitrary code execution. However, if the filename got wrapped in single quotes it failed, that is until now.

- [Link](#)

—

" "Thu, 28 Dec 2023

***Lot Reservation Management System 1.0 Shell Upload***

Lot Reservation Management System version 1.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

" "Thu, 28 Dec 2023

***Lot Reservation Management System 1.0 File Disclosure***

Lot Reservation Management System version 1.0 suffers from a file disclosure vulnerability.

- [Link](#)

—

" "Wed, 27 Dec 2023

***WhatACart 2.0.7 Cross Site Scripting***

WhatACart version 2.0.7 suffers from a cross site scripting vulnerability.

- [Link](#)

—

" "Tue, 26 Dec 2023

***ShopSite 14.0 Cross Site Scripting***

ShopSite version 14.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 26 Dec 2023

***FreeSWITCH 1.10.10 Denial Of Service***

When handling DTLS-SRTP for media setup, FreeSWITCH version 1.10.10 is susceptible to denial of service due to a race condition in the hello handshake phase of the DTLS protocol. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack.

- [Link](#)

—

” “Fri, 22 Dec 2023

***Craft CMS 4.4.14 Remote Code Execution***

This Metasploit module exploits an unauthenticated remote code execution vulnerability in Craft CMS versions 4.0.0-RC1 through 4.4.14.

- [Link](#)

—

” “Fri, 22 Dec 2023

***Hospital Management System 4.0 XSS / Shell Upload / SQL Injection***

Hospital Management System versions 4.0 and below suffer from cross site scripting, remote shell upload, and remote SQL injection vulnerabilities.

- [Link](#)

—

” “Fri, 22 Dec 2023

***GilaCMS 1.15.4 SQL Injection***

GilaCMS versions 1.15.4 and below suffer from multiple remote SQL injection vulnerabilities.

- [Link](#)

—

” “Thu, 21 Dec 2023

***Vinchin Backup And Recovery Command Injection***

This Metasploit module exploits a command injection vulnerability in Vinchin Backup & Recovery v5.0., v6.0., v6.7., and v7.0.. Due to insufficient input validation in the checkIpExists API endpoint, an attacker can execute arbitrary commands as the web server user.

- [Link](#)

—

” “Thu, 21 Dec 2023

***Glibc Tunables Privilege Escalation***

A buffer overflow exists in the GNU C Library’s dynamic loader ld.so while processing the GLIBC\_TUNABLES environment variable. It has been dubbed Looney Tunables. This issue allows a local attacker to use maliciously crafted GLIBC\_TUNABLES when launching binaries with



SUID permission to execute code in the context of the root user. This Metasploit module targets glibc packaged on Ubuntu and Debian. Fedora 37 and 38 and other distributions of linux also come packaged with versions of glibc vulnerable to CVE-2023-4911 however this module does not target them.

- [Link](#)

—  
”

## 4.2 0-Days der letzten 5 Tage

“Fri, 05 Jan 2024

**ZDI-24-018: Inductive Automation Ignition ExtendedDocumentCodec Deserialization of Untrusted Data Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 05 Jan 2024

**ZDI-24-017: Inductive Automation Ignition ResponseParser Notification Deserialization of Untrusted Data Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 05 Jan 2024

**ZDI-24-016: Inductive Automation Ignition ResponseParser SerializedResponse Deserialization of Untrusted Data Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 05 Jan 2024

**ZDI-24-015: Inductive Automation Ignition Base64Element Deserialization of Untrusted Data Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 05 Jan 2024

**ZDI-24-014: Inductive Automation Ignition RunQuery Deserialization of Untrusted Data Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-013: oFono SMS Decoder Stack-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-012: X.Org Server ProcXChangeProperty Heap-based Buffer Overflow Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-011: X.Org Server RecalculateMasterButtons Out-Of-Bounds Access Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-010: X.Org Server DeepCopyPointerClasses Out-Of-Bounds Access Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-009: X.Org Server RRChangeOutputProperty Integer Overflow Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-008: SolarWinds Access Rights Manager Hardcoded Credentials Authentication Bypass Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-007: Kofax Power PDF BMP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

**ZDI-24-006: Kofax Power PDF OXPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Thu, 04 Jan 2024

***ZDI-24-005: Kofax Power PDF OXPS File Parsing Use-After-Free Information Disclosure Vulnerability***

- [Link](#)

—

” “Thu, 04 Jan 2024

***ZDI-24-004: Kofax Power PDF OXPS File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Thu, 04 Jan 2024

***ZDI-24-003: Kofax Power PDF XPS File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

—

” “Thu, 04 Jan 2024

***ZDI-24-002: Kofax Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Thu, 04 Jan 2024

***ZDI-24-001: Kofax Power PDF XPS File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

—

”

## **5 Die Hacks der Woche**

mit Martin Haunschmid

### 5.0.1 Ihr habt WAS in eure Züge programmiert!?



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Jan)

Datum	Opfer	Land	Information
2024-01-04	City of Beckley	[USA]	<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
2024-01-06	[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>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-01-01	[Aspiration Training]	rhysida	Link
2024-01-01	[Southeast Vermont Transit (MOOver)]	bianlian	Link

## 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.