

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241006



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	11
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>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 Ein Grund mehr, Drucker zu hassen. Und Autos. . . . .	18
<b>6 Cyberangriffe: (Okt)</b>	<b>19</b>
<b>7 Ransomware-Erpressungen: (Okt)</b>	<b>19</b>
<b>8 Quellen</b>	<b>22</b>
8.1 Quellenverzeichnis . . . . .	22
<b>9 Impressum</b>	<b>23</b>

## 1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

#### ***Sicherheitsupdates: Cisco patcht Lücken in Produkten quer durch die Bank***

Neben einem kritischen Fehler kümmert sich der Netzwerkausrüster auch um einige Lücken mit mittlerem und hohem Risikograd. Patches stehen bereit.

- [Link](#)

—

#### ***Zimbra: Codeschmuggel-Lücke wird angegriffen***

In der Kollaborationssoftware Zimbra klafft eine Sicherheitslücke, die Angreifer bereits aktiv missbrauchen. Admins sollten zügig updaten.

- [Link](#)

—

#### ***Web-Config von Seiko-Epson-Geräten ermöglicht Angreifern Übernahme***

Das Web-Interface von Geräten wie Druckern von Seiko-Epson ermöglicht Angreifern in vielen Fällen, diese als Administrator zu übernehmen.

- [Link](#)

—

#### ***CERT-Bund warnt: Mehr als 15.000 Exchange-Server mit Sicherheitslücken***

In Deutschland stehen noch immer mehr als 15.000 Exchange-Server mit mindestens einer Codeschmuggel-Lücke offen im Netz, warnt das CERT-Bund.

- [Link](#)

—

#### ***Monitoring-Software Whatsup Gold: Hersteller rät zum schleunigen Update***

Progress warnt, dass teils kritische Sicherheitslücken in Whatsup Gold lauern. Admins sollen so schnell wie möglich aktualisieren.

- [Link](#)

—

#### ***Kritische Sicherheitslücken: PHP 8.3.12, 8.2.24 und 8.1.30 dichten Lecks ab***

Die PHP-Entwickler haben PHP 8.3.12, 8.2.24 und 8.1.30 veröffentlicht. Darin schließen sie mehrere, teils kritische Sicherheitslücken.

- [Link](#)

—

#### ***Foxit PDF: Manipulierte PDFs können Schadcode durchschleusen***

Es sind gegen verschiedene Attacken gerüstete Versionen von Foxit PDF Editor und PDF Reader für macOS und Windows erschienen.

- [Link](#)

---

**Teils kritische Lücken in Unix-Drucksystem CUPS ermöglichen Codeschmuggel**

Im Linux-Drucksystem CUPS wurden teils kritische Sicherheitslücken entdeckt. Angreifer können dadurch etwa Code einschmuggeln.

- [Link](#)

---

**Schadcode-Schlupfloch in Nvidia Container Toolkit geschlossen**

Angreifer können an Sicherheitslücken in Nvidia Container Toolkit und GPU Operator ansetzen, um Systeme zu kompromittieren.

- [Link](#)

---

**Sicherheitsupdates: DoS-Angriffe auf Cisco-Netzwerkhardware möglich**

Aufgrund von mehreren Sicherheitslücken in Ciscos Netzwerkbetriebssystem IOS XE sind verschiedene Geräte verwundbar. Patches stehen zum Download.

- [Link](#)

---

### 3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

#### 3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-7028	0.957580000	0.994830000	<a href="#">Link</a>
CVE-2023-6895	0.927330000	0.990820000	<a href="#">Link</a>
CVE-2023-6553	0.947820000	0.993190000	<a href="#">Link</a>
CVE-2023-6019	0.933510000	0.991420000	<a href="#">Link</a>
CVE-2023-52251	0.949200000	0.993390000	<a href="#">Link</a>
CVE-2023-4966	0.970840000	0.998170000	<a href="#">Link</a>
CVE-2023-49103	0.949680000	0.993480000	<a href="#">Link</a>
CVE-2023-48795	0.964670000	0.996220000	<a href="#">Link</a>
CVE-2023-47246	0.960360000	0.995270000	<a href="#">Link</a>
CVE-2023-46805	0.960890000	0.995400000	<a href="#">Link</a>
CVE-2023-46747	0.971540000	0.998420000	<a href="#">Link</a>
CVE-2023-46604	0.970850000	0.998180000	<a href="#">Link</a>
CVE-2023-4542	0.944110000	0.992630000	<a href="#">Link</a>
CVE-2023-43208	0.974060000	0.999430000	<a href="#">Link</a>
CVE-2023-43177	0.958390000	0.994960000	<a href="#">Link</a>
CVE-2023-42793	0.970970000	0.998230000	<a href="#">Link</a>
CVE-2023-41892	0.904950000	0.989050000	<a href="#">Link</a>
CVE-2023-41265	0.907590000	0.989240000	<a href="#">Link</a>
CVE-2023-39143	0.940700000	0.992230000	<a href="#">Link</a>
CVE-2023-38205	0.951890000	0.993850000	<a href="#">Link</a>
CVE-2023-38203	0.964750000	0.996270000	<a href="#">Link</a>
CVE-2023-38146	0.919150000	0.990030000	<a href="#">Link</a>
CVE-2023-38035	0.974600000	0.999680000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967920000	0.997190000	<a href="#">Link</a>
CVE-2023-3519	0.965910000	0.996610000	<a href="#">Link</a>
CVE-2023-35082	0.967900000	0.997180000	<a href="#">Link</a>
CVE-2023-35078	0.969440000	0.997620000	<a href="#">Link</a>
CVE-2023-34993	0.973450000	0.999160000	<a href="#">Link</a>
CVE-2023-34960	0.900520000	0.988790000	<a href="#">Link</a>
CVE-2023-34634	0.923140000	0.990410000	<a href="#">Link</a>
CVE-2023-34362	0.970450000	0.998030000	<a href="#">Link</a>
CVE-2023-34105	0.927500000	0.990840000	<a href="#">Link</a>
CVE-2023-34039	0.943770000	0.992580000	<a href="#">Link</a>
CVE-2023-3368	0.934610000	0.991540000	<a href="#">Link</a>
CVE-2023-33246	0.969870000	0.997810000	<a href="#">Link</a>
CVE-2023-32315	0.971490000	0.998400000	<a href="#">Link</a>
CVE-2023-30625	0.953820000	0.994230000	<a href="#">Link</a>
CVE-2023-30013	0.965950000	0.996620000	<a href="#">Link</a>
CVE-2023-29300	0.967820000	0.997140000	<a href="#">Link</a>
CVE-2023-29298	0.969430000	0.997620000	<a href="#">Link</a>
CVE-2023-28432	0.921930000	0.990300000	<a href="#">Link</a>
CVE-2023-28343	0.957650000	0.994840000	<a href="#">Link</a>
CVE-2023-28121	0.922260000	0.990330000	<a href="#">Link</a>
CVE-2023-27524	0.969670000	0.997700000	<a href="#">Link</a>
CVE-2023-27372	0.973980000	0.999410000	<a href="#">Link</a>
CVE-2023-27350	0.968980000	0.997480000	<a href="#">Link</a>
CVE-2023-26469	0.953540000	0.994160000	<a href="#">Link</a>
CVE-2023-26360	0.964630000	0.996210000	<a href="#">Link</a>
CVE-2023-26035	0.967750000	0.997120000	<a href="#">Link</a>
CVE-2023-25717	0.950620000	0.993610000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.964550000	0.996180000	<a href="#">Link</a>
CVE-2023-2479	0.963230000	0.995850000	<a href="#">Link</a>
CVE-2023-24489	0.972860000	0.998920000	<a href="#">Link</a>
CVE-2023-23752	0.952050000	0.993890000	<a href="#">Link</a>
CVE-2023-23333	0.960430000	0.995290000	<a href="#">Link</a>
CVE-2023-22527	0.970500000	0.998040000	<a href="#">Link</a>
CVE-2023-22518	0.959950000	0.995230000	<a href="#">Link</a>
CVE-2023-22515	0.973910000	0.999360000	<a href="#">Link</a>
CVE-2023-21839	0.947720000	0.993170000	<a href="#">Link</a>
CVE-2023-21554	0.952650000	0.994020000	<a href="#">Link</a>
CVE-2023-20887	0.970950000	0.998230000	<a href="#">Link</a>
CVE-2023-1698	0.917150000	0.989860000	<a href="#">Link</a>
CVE-2023-1671	0.962220000	0.995640000	<a href="#">Link</a>
CVE-2023-0669	0.971830000	0.998500000	<a href="#">Link</a>

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

Fri, 04 Oct 2024

**[NEU] [hoch] Xerox FreeFlow Core: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Core ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 04 Oct 2024

**[NEU] [UNGEPATCHT] [hoch] Cisco Small Business: Mehrere Schwachstellen ermöglichen Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Cisco Small Business ausnutzen, um seine Privilegien zu erhöhen, beliebige Befehle auszuführen und einen Denial of Service-Zustand zu verursachen.



- [Link](#)

—

Fri, 04 Oct 2024

***[NEU] [hoch] Cisco Nexus Dashboard und Nexus Dashboard Fabric Controller: Mehrere Schwachstellen***

Ein entfernter Angreifer kann mehrere Schwachstellen in Cisco Nexus Dashboard ausnutzen, um Informationen offenzulegen Sicherheitsmaßnahmen zu umgehen und beliebigen Code, im schlimmsten Fall mit Administratorrechten, zur Ausführung zu bringen.

- [Link](#)

—

Fri, 04 Oct 2024

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

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Jenkins und verschiedenen Jenkins Plugins ausnutzen, um Informationen offenzulegen Sicherheitsvorkehrungen zu umgehen oder seine Rechte zu erweitern.

- [Link](#)

—

Fri, 04 Oct 2024

***[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 04 Oct 2024

***[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 04 Oct 2024

***[NEU] [hoch] CUPS: Schwachstelle ermöglicht Denial of Service***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS cups-browsed ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 04 Oct 2024

***[UPDATE] [hoch] CUPS: Mehrere Schwachstellen ermöglichen Ausführung von beliebigem Programmcode***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in CUPS ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen und um Informationen offenzulegen.

- [Link](#)

—

Fri, 04 Oct 2024

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

Ein Angreifer kann mehrere Schwachstellen in ImageMagick ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Daten einzusehen oder weitere Angriffe mit nicht beschriebenen Auswirkungen durchzuführen.

- [Link](#)

—

Fri, 04 Oct 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, 04 Oct 2024

***[UPDATE] [hoch] UnZip: Mehrere Schwachstellen ermöglichen Codeausführung***

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

- [Link](#)

—

Fri, 04 Oct 2024

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

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

- [Link](#)

—

Fri, 04 Oct 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Fri, 04 Oct 2024

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

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder Code auszuführen.

- [Link](#)

—

Fri, 04 Oct 2024

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

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

- [Link](#)

—

Fri, 04 Oct 2024

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

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

- [Link](#)

—

Fri, 04 Oct 2024

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

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

- [Link](#)

—

Fri, 04 Oct 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.

- [Link](#)

—

Fri, 04 Oct 2024

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

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen oder Daten zu manipulieren.

- [Link](#)

Fri, 04 Oct 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

**3.3 Sicherheitslücken Meldungen von Tenable**

Datum	Schwachstelle	Bewertung
10/4/2024	[Telerik UI for WPF < 2024.3.924 Multiple Vulnerabilities]	critical
10/4/2024	[AlmaLinux 9 : thunderbird (ALSA-2024:7552)]	critical
10/4/2024	[AlmaLinux 9 : firefox (ALSA-2024:7505)]	critical
10/4/2024	[Debian dsa-5783 : firefox-esr - security update]	critical
10/4/2024	[Amazon Linux AMI : amazon-ssm-agent (ALAS-2024-1948)]	critical
10/5/2024	[Fedora 40 : chromium (2024-452b60addf)]	high
10/5/2024	[SUSE SLES15 Security Update : openssl-3 (SUSE-SU-2024:3525-1)]	high
10/5/2024	[SUSE SLES15 Security Update : frr (SUSE-SU-2024:3524-1)]	high
10/5/2024	[FreeBSD : zeek – potential DoS vulnerability (fe7031d3-3000-4b43-9fa6-52c2b624b8f9)]	high
10/5/2024	[Debian dsa-5786 : gir1.2-gsf-1 - security update]	high
10/4/2024	[Notepad++ < 8.4.1 DLL hijacking vulnerability]	high
10/4/2024	[OpenJDK 8 <= 8u412 / 11.0.0 <= 11.0.23 / 17.0.0 <= 17.0.11 / 21.0.0 <= 21.0.3 / 22.0.0 <= 22.0.1 Multiple Vulnerabilities (2024-07-16)]	high
10/4/2024	[Debian dla-3910 : comerr-dev - security update]	high

Datum	Schwachstelle	Bewertung
10/4/2024	[Debian dsa-5784 : liboath-dev - security update]	high
10/4/2024	[Amazon Linux AMI : kernel (ALAS-2024-1947)]	high
10/4/2024	[Oracle Linux 7 : e2fsprogs (ELSA-2024-12704)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Fri, 04 Oct 2024

#### **ABB Cylon Aspect 3.07.02 Authenticated File Disclosure**

ABB Cylon Aspect version 3.07.02 suffers from an authenticated arbitrary file disclosure vulnerability. Input passed through the file GET parameter through the downloadDb.php script is not properly verified before being used to download database files. This can be exploited to disclose the contents of arbitrary and sensitive files via directory traversal attacks.

- [Link](#)

—

” “Fri, 04 Oct 2024

#### **TeamViewer Privilege Escalation**

Proof of concept code for a flaw in TeamViewer that enables an unprivileged user to load an arbitrary kernel driver into the system.

- [Link](#)

—

” “Fri, 04 Oct 2024

#### **MD-Pro 1.0.76 Shell Upload / SQL Injection**

MD-Pro version 1.0.76 suffers from remote SQL injection and shell upload vulnerabilities.

- [Link](#)

—

” “Fri, 04 Oct 2024

#### **Computer Laboratory Management System 2024 1.0 Cross Site Scripting**

Computer Laboratory Management System 2024 version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**Acronis Cyber Infrastructure 5.0.1-61 Cross Site Request Forgery**

Acronis Cyber Infrastructure version 5.0.1-61 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**Vehicle Service Management System 1.0 WYSIWYG Code Injection**

Vehicle Service Management System version 1.0 suffers from a WYSIWYG code injection vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**Vehicle Service Management System 1.0 Code Injection**

Vehicle Service Management System version 1.0 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**Transport Management System 1.0 Arbitrary File Upload**

Transport Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**Transport Management System 1.0 Code Injection**

Transport Management System version 1.0 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**ManageEngine ADManager 7183 Password Hash Disclosure**

ManageEngine ADManager version 7183 suffers from a password hash disclosure vulnerability.

- [Link](#)

—

” “Fri, 04 Oct 2024

**fastrpc\_mmap\_create Use-After-Free**

A condition exists when fastrpc\_mmap\_create creates a new globally visible mapping that can lead to a use-after-free.

- [Link](#)

—

” “Thu, 03 Oct 2024

**Acronis Cyber Infrastructure Default Password Remote Code Execution**

Acronis Cyber Infrastructure (ACI) is an IT infrastructure solution that provides storage, compute, and

network resources. Businesses and Service Providers are using it for data storage, backup storage, creating and managing virtual machines and software-defined networks, running cloud-native applications in production environments. This Metasploit module exploits a default password vulnerability in ACI which allow an attacker to access the ACI PostgreSQL database and gain administrative access to the ACI Web Portal. This opens the door for the attacker to upload SSH keys that enables root access to the appliance/server. This attack can be remotely executed over the WAN as long as the PostgreSQL and SSH services are exposed to the outside world. ACI versions 5.0 before build 5.0.1-61, 5.1 before build 5.1.1-71, 5.2 before build 5.2.1-69, 5.3 before build 5.3.1-53, and 5.4 before build 5.4.4-132 are vulnerable.

- [Link](#)

—

” “Thu, 03 Oct 2024

***dizqueTV 1.5.3 Remote Code Execution***

dizqueTV version 1.5.3 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***openSIS 9.1 SQL Injection***

openSIS version 9.1 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***reNgin 2.2.0 Command Injection***

reNgin version 2.2.0 suffers from an authenticated command injection vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***WordPress Bricks Builder Theme 1.9.6 Code Injection***

WordPress Bricks Builder Theme version 1.9.6 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***WordPress Hash Form 1.1.0 Code Injection***

WordPress Hash Form plugin version 1.1.0 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***WordPress GiveWP Donation Fundraising Platform 3.14.1 Code Injection***

WordPress GiveWP Donation Fundraising Platform version 3.14.1 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***ViciDial 2.0.5 Cross Site Request Forgery***

ViciDial version 2.0.5 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***Vehicle Service Management System 1.0 Cross Site Request Forgery***

Vehicle Service Management System version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***Transport Management System 1.0 Insecure Direct Object Reference***

Transport Management System version 1.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***Printing Business Records Management System 1.0 Insecure Settings***

Printing Business Records Management System version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***Online Eyewear Shop 1.0 Insecure Settings***

Online Eyewear Shop version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 03 Oct 2024

***AVideo 12.4 Code Injection***

AVideo version 12.4 suffers from a PHP code injection vulnerability.

- [Link](#)

—

” “Wed, 02 Oct 2024

***CUPS Arbitrary Command Execution***



Proof of concept remote command execution exploit for CUPS that leverages the vulnerability outlined in CVE-2024-47176.

- [Link](#)

—  
”

## 4.2 0-Days der letzten 5 Tage

“Wed, 02 Oct 2024

***ZDI-24-1321: Apple macOS AppleVADriver Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1320: Autodesk Navisworks Freedom DWF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1319: Autodesk Navisworks Freedom DWF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1318: Autodesk Navisworks Freedom DWFX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1317: Autodesk Navisworks Freedom DWFX File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1316: Autodesk Navisworks Freedom DWFX File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1315: Autodesk Navisworks Freedom DWF File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1314: PaperCut NG pc-web-print Link Following Denial-of-Service Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1313: Apple macOS ImageIO PSD File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1312: Apple macOS ImageIO KTX Image Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- [Link](#)

—

” “Wed, 02 Oct 2024

***ZDI-24-1311: Microsoft Windows Menu DC Path Use-After-Free Local Privilege Escalation Vulnerability***

- [Link](#)

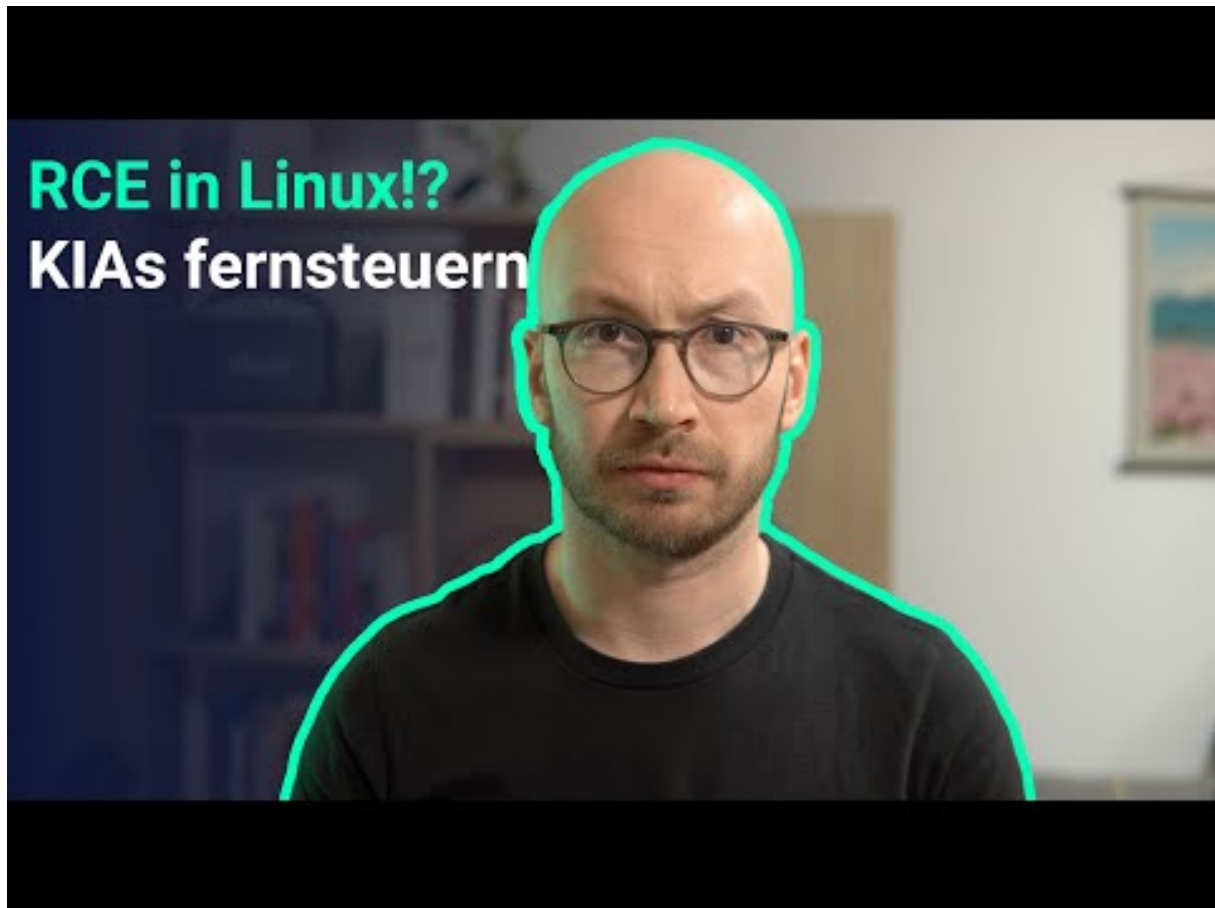
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Ein Grund mehr, Drucker zu hassen. Und Autos.



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Okt)

Datum	Opfer	Land	Information
2024-10-04	Groupe Hospi Grand Ouest	[FRA]	<a href="#">Link</a>
2024-10-03	Uttarakhand	[IND]	<a href="#">Link</a>
2024-10-02	Thoraxzentrum Bezirk Unterfranken	[DEU]	<a href="#">Link</a>
2024-10-02	Wayne County	[USA]	<a href="#">Link</a>
2024-10-01	Oyonnax	[FRA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Okt)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-05	[Creative Consumer Concepts]	play	<a href="#">Link</a>
2024-10-05	[Power Torque Services]	play	<a href="#">Link</a>
2024-10-05	[seoulpi.io]	killsec	<a href="#">Link</a>
2024-10-05	[canstarrestorations.com]	ransomhub	<a href="#">Link</a>
2024-10-05	[www.ravencm.com]	ransomhub	<a href="#">Link</a>
2024-10-05	[Ibermutuamur]	hunters	<a href="#">Link</a>
2024-10-05	[betterhalf.ai]	killsec	<a href="#">Link</a>
2024-10-05	[HARTSON-KENNEDY.COM]	clop	<a href="#">Link</a>
2024-10-04	[omniboxx.nl]	ransomhub	<a href="#">Link</a>
2024-10-05	[BNBuilders]	hunters	<a href="#">Link</a>
2024-10-04	[winwinza.com]	ransomhub	<a href="#">Link</a>
2024-10-04	[Storck-Baugesellschaft mbH]	incransom	<a href="#">Link</a>
2024-10-04	[C&L Ward]	play	<a href="#">Link</a>
2024-10-04	[Wilmington Convention Center]	play	<a href="#">Link</a>
2024-10-04	[Guerriere & Halnon]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-04	[Markdom Plastic Products]	play	<a href="#">Link</a>
2024-10-04	[Pete's Road Service]	play	<a href="#">Link</a>
2024-10-04	[release.io]	ransomhub	<a href="#">Link</a>
2024-10-04	[kleberandassociates.com]	ransomhub	<a href="#">Link</a>
2024-10-04	[City Of Forest Park - Full Leak]	monti	<a href="#">Link</a>
2024-10-04	[Riley Gear Corporation]	akira	<a href="#">Link</a>
2024-10-04	[TANYA Creations]	akira	<a href="#">Link</a>
2024-10-04	[mullenwylie.com]	ElDorado	<a href="#">Link</a>
2024-10-04	[GenPro Inc.]	blacksuit	<a href="#">Link</a>
2024-10-04	[CopySmart LLC]	ciphbit	<a href="#">Link</a>
2024-10-04	[North American Breaker]	akira	<a href="#">Link</a>
2024-10-04	[Amplitude Laser]	hunters	<a href="#">Link</a>
2024-10-04	[GW Mechanical]	hunters	<a href="#">Link</a>
2024-10-04	[Dreyfuss + Blackford Architecture]	hunters	<a href="#">Link</a>
2024-10-04	[Transtec SAS]	orca	<a href="#">Link</a>
2024-10-02	[enterpriseoutsourcing.com]	ransomhub	<a href="#">Link</a>
2024-10-04	[DPC DATA]	qilin	<a href="#">Link</a>
2024-10-03	[Lyomark Pharma]	dragonforce	<a href="#">Link</a>
2024-10-03	[Conductive Containers, Inc]	cicada3301	<a href="#">Link</a>
2024-10-04	[bbgc.gov.bd]	killsec	<a href="#">Link</a>
2024-10-03	[CobelPlast]	hunters	<a href="#">Link</a>
2024-10-03	[Shin Bet]	handala	<a href="#">Link</a>
2024-10-03	[Barnes & Cohen]	trinity	<a href="#">Link</a>
2024-10-03	[TRC Worldwide Engineering (Trcww)]	akira	<a href="#">Link</a>
2024-10-03	[Rob Levine & Associates (roblevine.com)]	akira	<a href="#">Link</a>
2024-10-03	[Red Barrels]	nitrogen	<a href="#">Link</a>
2024-10-03	[CaleyWray]	hunters	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-03	[LIFTING.COM]	clop	<a href="#">Link</a>
2024-10-01	[Emerson]	medusa	<a href="#">Link</a>
2024-10-03	[Golden Age Nursing Home]	rhysida	<a href="#">Link</a>
2024-10-02	[mccartycompany.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[bypeterandpauls.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[domainindustries.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[ironmetals.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[rollxvans.com]	ransomhub	<a href="#">Link</a>
2024-10-02	[ETC Companies]	akira	<a href="#">Link</a>
2024-10-02	[Branhaven Chrysler Dodge Jeep Ram]	blacksuit	<a href="#">Link</a>
2024-10-02	[Holmes & Brakel]	akira	<a href="#">Link</a>
2024-10-02	[Forshey Prostok LLP]	qilin	<a href="#">Link</a>
2024-10-02	[Israel Prime Minister Emails]	handala	<a href="#">Link</a>
2024-10-02	[FoccoERP]	trinity	<a href="#">Link</a>
2024-10-01	[Quantum Healthcare]	incransom	<a href="#">Link</a>
2024-10-01	[Acuity Advisor]	stormous	<a href="#">Link</a>
2024-10-01	[United Animal Health]	qilin	<a href="#">Link</a>
2024-10-01	[Akromold]	nitrogen	<a href="#">Link</a>
2024-10-01	[Labib Funk Associates]	nitrogen	<a href="#">Link</a>
2024-10-01	[Research Electronics International]	nitrogen	<a href="#">Link</a>
2024-10-01	[Cascade Columbia Distribution]	akira	<a href="#">Link</a>
2024-10-01	[ShoreMaster]	akira	<a href="#">Link</a>
2024-10-01	[marthamedeiros.com.br]	madliberator	<a href="#">Link</a>
2024-10-01	[CSG Consultants]	akira	<a href="#">Link</a>
2024-10-01	[aberdeenwa.gov]	ElDorado	<a href="#">Link</a>
2024-10-01	[Corantioquia]	meow	<a href="#">Link</a>
2024-10-01	[performance-therapies]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-10-01	[www.galab.com]	cactus	<a href="#">Link</a>
2024-10-01	[telehealthcenter.in]	killsec	<a href="#">Link</a>
2024-10-01	[howardcpas.com]	ElDorado	<a href="#">Link</a>
2024-10-01	[bshsoft.com]	ElDorado	<a href="#">Link</a>
2024-10-01	[credihealth.com]	killsec	<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.