

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241106



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	11
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>13</b>
4.1 Exploits der letzten 5 Tage . . . . .	13
4.2 0-Days der letzten 5 Tage . . . . .	18
<b>5 Die Hacks der Woche</b>	<b>19</b>
5.0.1 Sophos spielt die UNO Reverse Karte ☒ (+ Redline Stealer) . . . . .	19
<b>6 Cyberangriffe: (Nov)</b>	<b>20</b>
<b>7 Ransomware-Erpressungen: (Nov)</b>	<b>20</b>
<b>8 Quellen</b>	<b>22</b>
8.1 Quellenverzeichnis . . . . .	22
<b>9 Impressum</b>	<b>24</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

#### ***HPE Aruba stopft Codeschmuggel-Lücken in Access Points***

Firmware-Updates für HPE Aruba Access Points stopfen mehrere kritische Sicherheitslücken, die Angreifern das Einschleusen von Schadcode ermöglichen.

- [Link](#)

—

#### ***Synology korrigiert weitere kritische Pwn2Own-Sicherheitslücken***

Synology-NAS waren ein beliebtes Ziel beim Pwn2Own-Wettbewerb in Irland. Der Hersteller stopft weitere, dort entdeckte kritische Sicherheitslücken.

- [Link](#)

—

#### ***Veritas Netbackup: Rechteausweitung in Windows möglich***

Hersteller Veritas warnt vor einer Sicherheitslücke in Netbackup unter Windows. Angreifer können dadurch ihre Rechte ausweiten.

- [Link](#)

—

#### ***Android-Patchday: Updates stopfen zwei angegriffene Sicherheitslücken***

Der Android-Patchday im November bringt Aktualisierungen mit, die unter anderem zwei bereits angegriffene Sicherheitslecks abdichten.

- [Link](#)

—

#### ***Zoho ManageEngine ADManager Plus: Angreifer können SQL-Befehle einschleusen***

In ManageEngine ADManager Plus von Zohocorp können Angreifer eine SQL-Injection-Lücke missbrauchen und dadurch unbefugten Zugriff erlangen.

- [Link](#)

—

#### ***Okta: Sicherheitslücke in Verify gibt Angreifern Zugriff auf Passwörter***

In Verify von Okta können Angreifer eine Sicherheitslücke im Windows-Agent missbrauchen, um Passwörter abzugreifen. Eine weitere Lücke betrifft Okta AD/LDAP.

- [Link](#)

—

#### ***Sicherheitsupdates: Schadcode-Attacken auf Synology-NAS möglich***

Zwei während des Hackerwettbewerbs Pwn2Own entdeckte kritische Sicherheitslücken in NAS-Geräten von Synology wurden geschlossen.

- [Link](#)

---

***Nvidia ConnectX, BlueField: Angreifer können Daten manipulieren***

In aktuellen Firmwareversion hat Nvidia Sicherheitslücken im Netzwerkadapter ConnectX und der Computing-Plattform BlueField geschlossen.

- [Link](#)

---

***Jetzt patchen! Ransomware-Attacken auf Server mit CyberPanel beobachtet***

Angreifer nutzen kritische Schwachstellen in Servern aus, auf denen CyberPanel installiert ist. Eine abgesicherte Version ist verfügbar.

- [Link](#)

---

***Qnap schließt NAS-Sicherheitslücken aus Hackerwettbewerb***

NAS-Modelle von Qnap mit der Backupsoftware HBS 3 Hybrid Backup Sync sind angreifbar. Auch im SMB-Service wurde eine kritische Lücke geschlossen.

- [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	0.994990000	<a href="#">Link</a>
CVE-2023-6895	0.925010000	0.990870000	<a href="#">Link</a>
CVE-2023-6553	0.949860000	0.993720000	<a href="#">Link</a>
CVE-2023-6019	0.932040000	0.991530000	<a href="#">Link</a>
CVE-2023-6018	0.911590000	0.989850000	<a href="#">Link</a>
CVE-2023-52251	0.947690000	0.993410000	<a href="#">Link</a>
CVE-2023-4966	0.970850000	0.998240000	<a href="#">Link</a>
CVE-2023-49103	0.947920000	0.993430000	<a href="#">Link</a>
CVE-2023-48795	0.962520000	0.995820000	<a href="#">Link</a>
CVE-2023-47246	0.962070000	0.995740000	<a href="#">Link</a>
CVE-2023-46805	0.962030000	0.995730000	<a href="#">Link</a>
CVE-2023-46747	0.972770000	0.998910000	<a href="#">Link</a>
CVE-2023-46604	0.969640000	0.997780000	<a href="#">Link</a>
CVE-2023-4542	0.941060000	0.992560000	<a href="#">Link</a>
CVE-2023-43208	0.974790000	0.999780000	<a href="#">Link</a>
CVE-2023-43177	0.957850000	0.995030000	<a href="#">Link</a>
CVE-2023-42793	0.970830000	0.998240000	<a href="#">Link</a>
CVE-2023-41892	0.905460000	0.989410000	<a href="#">Link</a>
CVE-2023-41265	0.920970000	0.990490000	<a href="#">Link</a>
CVE-2023-38205	0.955500000	0.994620000	<a href="#">Link</a>
CVE-2023-38203	0.964750000	0.996340000	<a href="#">Link</a>
CVE-2023-38146	0.920950000	0.990490000	<a href="#">Link</a>
CVE-2023-38035	0.974570000	0.999680000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.967260000	0.997050000	<a href="#">Link</a>
CVE-2023-3519	0.965540000	0.996590000	<a href="#">Link</a>
CVE-2023-35082	0.965310000	0.996530000	<a href="#">Link</a>
CVE-2023-35078	0.967840000	0.997230000	<a href="#">Link</a>
CVE-2023-34993	0.973050000	0.999020000	<a href="#">Link</a>
CVE-2023-34634	0.926130000	0.990970000	<a href="#">Link</a>
CVE-2023-34362	0.969990000	0.997940000	<a href="#">Link</a>
CVE-2023-34039	0.944770000	0.993030000	<a href="#">Link</a>
CVE-2023-3368	0.928640000	0.991200000	<a href="#">Link</a>
CVE-2023-33246	0.973040000	0.999010000	<a href="#">Link</a>
CVE-2023-32315	0.973320000	0.999130000	<a href="#">Link</a>
CVE-2023-30625	0.953680000	0.994320000	<a href="#">Link</a>
CVE-2023-30013	0.962230000	0.995760000	<a href="#">Link</a>
CVE-2023-29300	0.967820000	0.997220000	<a href="#">Link</a>
CVE-2023-29298	0.968120000	0.997330000	<a href="#">Link</a>
CVE-2023-28432	0.921730000	0.990580000	<a href="#">Link</a>
CVE-2023-28343	0.962760000	0.995880000	<a href="#">Link</a>
CVE-2023-28121	0.927310000	0.991080000	<a href="#">Link</a>
CVE-2023-27524	0.970490000	0.998120000	<a href="#">Link</a>
CVE-2023-27372	0.973760000	0.999330000	<a href="#">Link</a>
CVE-2023-27350	0.969490000	0.997740000	<a href="#">Link</a>
CVE-2023-26469	0.955890000	0.994680000	<a href="#">Link</a>
CVE-2023-26360	0.963280000	0.995990000	<a href="#">Link</a>
CVE-2023-26035	0.969120000	0.997620000	<a href="#">Link</a>
CVE-2023-25717	0.950620000	0.993810000	<a href="#">Link</a>
CVE-2023-25194	0.965880000	0.996690000	<a href="#">Link</a>
CVE-2023-2479	0.961940000	0.995710000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-24489	0.972720000	0.998870000	<a href="#">Link</a>
CVE-2023-23752	0.949040000	0.993580000	<a href="#">Link</a>
CVE-2023-23397	0.902750000	0.989280000	<a href="#">Link</a>
CVE-2023-23333	0.963480000	0.996040000	<a href="#">Link</a>
CVE-2023-22527	0.970950000	0.998300000	<a href="#">Link</a>
CVE-2023-22518	0.965000000	0.996410000	<a href="#">Link</a>
CVE-2023-22515	0.973100000	0.999040000	<a href="#">Link</a>
CVE-2023-21839	0.933960000	0.991770000	<a href="#">Link</a>
CVE-2023-21554	0.955110000	0.994540000	<a href="#">Link</a>
CVE-2023-20887	0.970370000	0.998070000	<a href="#">Link</a>
CVE-2023-1698	0.916400000	0.990120000	<a href="#">Link</a>
CVE-2023-1671	0.962340000	0.995800000	<a href="#">Link</a>
CVE-2023-0669	0.971830000	0.998560000	<a href="#">Link</a>

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

Tue, 05 Nov 2024

**[NEU] [hoch] Red Hat Enterprise Linux (OpenEXR): Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Tue, 05 Nov 2024

**[NEU] [hoch] Microsoft NuGet: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft NuGet ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—



Tue, 05 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 05 Nov 2024

**[NEU] [hoch] Android Patchday November 2024**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [hoch] OpenJPEG: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenJPEG ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [hoch] Red Hat OpenStack: Schwachstelle ermöglicht Erlangung erweiterter Privilegien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenStack ausnutzen, um erweiterte Privilegien zu erlangen.

- [Link](#)

—

Tue, 05 Nov 2024

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

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Tue, 05 Nov 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](#)

—

Tue, 05 Nov 2024

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

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

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [hoch] Apache Camel und mehrere Red Hat Produkte: Mehrere Schwachstellen**

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Apache Camel und in mehreren Red Hat-Produkten ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben und beliebigen Code auszuführen.

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [hoch] Mozilla Firefox, ESR und Thunderbird: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [hoch] X.Org X11 und Xming: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in X.Org X11 und Xming ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

—

Tue, 05 Nov 2024

**[UPDATE] [UNGEPATCHT] [kritisch] DrayTek Vigor: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter anonymer oder authentifizierter Angreifer kann mehrere Schwachstellen in DrayTek Vigor ausnutzen, um beliebigen Code auszuführen.

- [Link](#)

—

Mon, 04 Nov 2024

**[NEU] [hoch] Red Hat Enterprise Linux (xerces-c): Schwachstelle ermöglicht Codeausführung, Offenlegung von Informationen oder DoS**

Ein entfernter, authentifizierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Mon, 04 Nov 2024

**[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Mon, 04 Nov 2024

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

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

- [Link](#)

—

Mon, 04 Nov 2024

**[UPDATE] [hoch] IBM WebSphere Application Server: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in IBM WebSphere Application Server ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Mon, 04 Nov 2024

**[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Mon, 04 Nov 2024

**[UPDATE] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in docker ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
11/5/2024	[Fedora 40 : llama-cpp (2024-b07b0b41ec)]	critical
11/5/2024	[PTZOptics Camera Multiple Vulnerabilities (Direct Check)]	critical
11/5/2024	[Oracle Business Intelligence Enterprise Edition (October 2024 CPU)]	critical
11/5/2024	[Oracle Business Intelligence Enterprise Edition (OAS 7.6) (October 2024 CPU)]	critical
11/5/2024	[Oracle Business Intelligence Enterprise Edition (OAS 7.0) (October 2024 CPU)]	critical
11/5/2024	[RHEL 7 : krb5 (RHSA-2024:8788)]	critical
11/5/2024	[Oracle Business Intelligence Publisher 6.4 / 7.0 (OAS) (October 2024 CPU)]	critical
11/5/2024	[RHEL 8 : krb5 (RHSA-2024:8792)]	critical
11/5/2024	[RHEL 8 : krb5 (RHSA-2024:8791)]	critical
11/5/2024	[RHEL 8 : xmlrpc-c (RHSA-2024:8859)]	critical
11/5/2024	[RHEL 8 : krb5 (RHSA-2024:8860)]	critical
11/5/2024	[RHEL 9 : openexr (RHSA-2024:8800)]	critical
11/5/2024	[FreeBSD : libqb – Buffer overflow (ecf9a798-9aa9-11ef-a8f0-a8a15998b5cb)]	critical
11/5/2024	[Google Chrome < 130.0.6723.116 Multiple Vulnerabilities]	critical
11/5/2024	[Google Chrome < 130.0.6723.117 Multiple Vulnerabilities]	critical

Datum	Schwachstelle	Bewertung
11/5/2024	[Google Chrome < 130.0.6723.116 Multiple Vulnerabilities]	critical
11/5/2024	[Oracle Linux 8 : python-gevent (ELSA-2024-8834)]	critical
11/5/2024	[Fedora 40 : python-quart (2024-51bff89a25)]	high
11/5/2024	[Ubuntu 22.04 LTS / 24.04 LTS / 24.10 : Ruby vulnerabilities (USN-7091-1)]	high
11/5/2024	[Oracle E-Business Suite (October 2024 CPU)]	high
11/5/2024	[RHEL 8 : Red Hat JBoss Enterprise Application Platform 8.0.4 Security update (Important) (RHSA-2024:8823)]	high
11/5/2024	[RHEL 9 : thunderbird (RHSA-2024:8793)]	high
11/5/2024	[Oracle Business Intelligence Publisher (October 2024 CPU)]	high
11/5/2024	[Oracle Business Process Management Suite (October 2024 CPU)]	high
11/5/2024	[RHEL 8 : python3.11 (RHSA-2024:8838)]	high
11/5/2024	[RHEL 8 : python3.12 (RHSA-2024:8836)]	high
11/5/2024	[RHEL 8 : haproxy (RHSA-2024:8849)]	high
11/5/2024	[RHEL 8 : libtiff (RHSA-2024:8833)]	high
11/5/2024	[RHEL 8 : kernel-rt (RHSA-2024:8870)]	high
11/5/2024	[RHEL 8 : Red Hat Product OCP Tools 4.13 Openshift Jenkins (RHSA-2024:8887)]	high
11/5/2024	[RHEL 8 : Red Hat Product OCP Tools 4.14 Openshift Jenkins (RHSA-2024:8885)]	high
11/5/2024	[RHEL 8 : Red Hat Product OCP Tools 4.12 Openshift Jenkins (RHSA-2024:8886)]	high
11/5/2024	[RHEL 8 : Red Hat Product OCP Tools 4.15 Openshift Jenkins (RHSA-2024:8884)]	high
11/5/2024	[Debian dsa-5803 : thunderbird - security update]	high
11/5/2024	[Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2024-12806)]	high

Datum	Schwachstelle	Bewertung
11/5/2024	[Ubuntu 22.04 LTS / 24.04 LTS / 24.10 : Werkzeug vulnerability (USN-7093-1)]	high
11/5/2024	[Debian dla-3945 : heif-gdk-pixbuf - security update]	high
11/5/2024	[Debian dla-3946 : context - security update]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Tue, 05 Nov 2024

#### **ABB Cylon Aspect 3.08.00 Off-By-One**

A vulnerability was identified in a ABB Cylon Aspect version 3.08.00 where an off-by-one error in array access could lead to undefined behavior and potential denial of service. The issue arises in a loop that iterates over an array using a less than or equals to condition, allowing access to an out-of-bounds index. This can trigger errors or unexpected behavior when processing data, potentially crashing the application. Successful exploitation of this vulnerability can lead to a crash or disruption of service, especially if the script handles large data sets.

- [Link](#)

—

” “Mon, 04 Nov 2024

#### **Sysax Multi Server 6.99 SSH Denial Of Service**

Sysax Multi Server version 6.9.9 suffers from an SSH related denial of service vulnerability.

- [Link](#)

—

” “Mon, 04 Nov 2024

#### **Sysax Multi Server 6.99 Cross Site Scripting**

Sysax Multi Server version 6.9.9 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 04 Nov 2024

#### **IBM Security Verify Access 32 Vulnerabilities**

IBM Security Verify Access versions prior to 10.0.8 suffer from authentication bypass, reuse of private keys, local privilege escalation, weak settings, outdated libraries, missing password, hardcoded secrets, remote code execution, missing authentication, null pointer dereference, and lack of privilege

separation vulnerabilities.

- [Link](#)

—

” “Mon, 04 Nov 2024

***IBM Security Verify Access Appliance Insecure Transit / Hardcoded Passwords***

IBM Security Verify Access Appliance suffers from multiple insecure transit vulnerabilities, hardcoded passwords, and uninitialized variables. ibmsecurity versions prior to 2024.4.5 are affected.

- [Link](#)

—

” “Mon, 04 Nov 2024

***ESET NOD32 Antivirus 18.0.12.0 Unquoted Service Path***

ESET NOD32 Antivirus version 18.0.12.0 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Mon, 04 Nov 2024

***SQLite3 generate\_series Stack Buffer Underflow***

SQLite3 suffers from a stack buffer underflow condition in seriesBestIndex in the generate\_series extension.

- [Link](#)

—

” “Mon, 04 Nov 2024

***Linux khugepaged Race Conditions***

khugepaged in Linux races with rmap-based zap, races with GUP-fast, and fails to call MMU notifiers.

- [Link](#)

—

” “Fri, 01 Nov 2024

***Ping Identity PingIDM 7.5.0 Query Filter Injection***

Ping Identity PingIDM versions 7.0.0 through 7.5.0 enabled an attacker with read access to the User collection, to abuse API query filters in order to obtain managed and/or internal user's passwords in either plaintext or encrypted variants, based on configuration. The API clearly prevents the password in either plaintext or encrypted to be retrieved by any other means, as this field is set as protected under the User object. However, by injecting a malicious query filter, using password as the field to be filtered, an attacker can perform a blind brute-force on any victim's user password details (encrypted object or plaintext string).

- [Link](#)

—

” “Fri, 01 Nov 2024

***ABB Cylon Aspect 3.08.01 File Upload MD5 Checksum Bypass***

ABB Cylon Aspect version 3.08.01 has a vulnerability in caldavInstall.php, caldavInstallAgendav.php, and caldavUpload.php files, where the presence of an EXPERTMODE parameter activates a badass-Mode feature. This mode allows an unauthenticated attacker to bypass MD5 checksum validation during file uploads. By enabling badassMode and setting the skipChecksum parameter, the system skips integrity verification, allowing attackers to upload or install altered CalDAV zip files without authentication. This vulnerability permits unauthorized file modifications, potentially exposing the system to tampering or malicious uploads.

- [Link](#)

—

” “Fri, 01 Nov 2024

#### ***Packet Storm New Exploits For October, 2024***

This archive contains all of the 128 exploits added to Packet Storm in October, 2024.

- [Link](#)

—

” “Fri, 01 Nov 2024

#### ***SmartAgent 1.1.0 Remote Code Execution***

SmartAgent version 1.1.0 suffers from an unauthenticated remote code execution vulnerability in youtubeInfo.php.

- [Link](#)

—

” “Fri, 01 Nov 2024

#### ***SmartAgent 1.1.0 Server-Side Request Forgery***

SmartAgent version 1.1.0 suffers from a server-side request forgery vulnerability.

- [Link](#)

—

” “Fri, 01 Nov 2024

#### ***SmartAgent 1.1.0 SQL Injection***

SmartAgent version 1.1.0 suffers from multiple unauthenticated remote SQL injection vulnerabilities.

- [Link](#)

—

” “Thu, 31 Oct 2024

#### ***WordPress Automatic 3.92.0 Path Traversal / Server-Side Request Forgery***

WordPress Automatic plugin versions 3.92.0 and below proof of concept exploit that demonstrates path traversal and server-side request forgery vulnerabilities.

- [Link](#)

—

” “Thu, 31 Oct 2024

#### ***Qualitor 8.24 Server-Side Request Forgery***



Qualitor versions 8.24 and below suffer from an unauthenticated server-side request forgery vulnerability.

- [Link](#)

—

” “Thu, 31 Oct 2024

#### ***CyberPanel Command Injection***

Proof of concept exploit for a command injection vulnerability in CyberPanel. This vulnerability enables unauthenticated attackers to inject and execute arbitrary commands on vulnerable servers by sending crafted OPTIONS HTTP requests to /dns/getresetstatus and /ftp/getresetstatus endpoints, potentially leading to full system compromise. Versions prior to 1c0c6cb appear to be affected.

- [Link](#)

—

” “Thu, 31 Oct 2024

#### ***Skyhigh Client Proxy Policy Bypass***

Proof of concept code for a flaw where a malicious insider can bypass the existing policy of Skyhigh Client Proxy without a valid release code.

- [Link](#)

—

” “Wed, 30 Oct 2024

#### ***WordPress WP-Automatic SQL Injection***

This Metasploit module exploits an unauthenticated SQL injection vulnerability in the WordPress wp-automatic plugin versions prior to 3.92.1 to achieve remote code execution. The vulnerability allows the attacker to inject and execute arbitrary SQL commands, which can be used to create a malicious administrator account. The password for the new account is hashed using MD5. Once the administrator account is created, the attacker can upload and execute a malicious plugin, leading to full control over the WordPress site.

- [Link](#)

—

” “Wed, 30 Oct 2024

#### ***ABB Cylon Aspect 3.08.01 jsonProxy.php Username Enumeration***

ABB Cylon Aspect version 3.08.01 is vulnerable to username enumeration in the jsonProxy.php endpoint. An unauthenticated attacker can interact with the UserManager servlet to enumerate valid usernames on the system. Since jsonProxy.php proxies requests to internal services without requiring authentication, attackers can gain unauthorized insights into valid usernames.

- [Link](#)

—

” “Wed, 30 Oct 2024

#### ***ABB Cylon Aspect 3.08.01 jsonProxy.php Information Disclosure***

ABB Cylon Aspect version 3.08.01 is vulnerable to unauthorized information disclosure in the jsonProxy.php endpoint. An unauthenticated attacker can retrieve sensitive system information, including system time, uptime, memory usage, and network load statistics. The jsonProxy.php endpoint proxies these requests to internal services without requiring authentication, allowing attackers to obtain detailed system status data, which could aid in further attacks by revealing operational characteristics and resource utilization.

- [Link](#)

—

” “Wed, 30 Oct 2024

***ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Remote SSH Service Control***

ABB Cylon Aspect version 3.08.01 is vulnerable to unauthorized SSH service configuration changes via the jsonProxy.php endpoint. An unauthenticated attacker can enable or disable the SSH service on the server by accessing the FTControlServlet with the sshenable parameter. The jsonProxy.php script proxies requests to localhost without enforcing authentication, allowing attackers to modify SSH settings and potentially gain further unauthorized access to the system.

- [Link](#)

—

” “Wed, 30 Oct 2024

***ABB Cylon Aspect 3.08.01 jsonProxy.php Denial Of Service***

ABB Cylon Aspect version 3.08.01 is vulnerable to an unauthenticated denial of service attack in the jsonProxy.php endpoint. An attacker can remotely restart the main Java server by accessing the FTControlServlet with the restart parameter. The endpoint proxies requests to localhost without requiring authentication, enabling attackers to disrupt system availability by repeatedly triggering server restarts.

- [Link](#)

—

” “Wed, 30 Oct 2024

***ABB Cylon Aspect 3.08.01 jsonProxy.php Unauthenticated Project Download***

ABB Cylon Aspect version 3.08.01 is vulnerable to an unauthorized project file disclosure in jsonProxy.php. An unauthenticated remote attacker can issue a GET request abusing the DownloadProject servlet to download sensitive project files. The jsonProxy.php script bypasses authentication by proxying requests to localhost (AspectFT Automation Application Server), granting remote attackers unauthorized access to internal Java servlets. This exposes potentially sensitive project data and configuration details without requiring authentication.

- [Link](#)

—

” “Wed, 30 Oct 2024

***ABB Cylon Aspect 3.08.01 jsonProxy.php Servlet Inclusion Authentication Bypass***

ABB Cylon Aspect version 3.08.01 is vulnerable to remote, arbitrary servlet inclusion. The jsonProxy.php endpoint allows unauthenticated remote attackers to access internal services by proxying requests to localhost. This results in an authentication bypass, enabling attackers to interact with multiple java servlets without authorization, potentially exposing sensitive system functions and information.

- [Link](#)

—  
”

## 4.2 0-Days der letzten 5 Tage

“Tue, 05 Nov 2024

**ZDI-24-1456: Linux Kernel ksmbd Session Race Condition Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 05 Nov 2024

**ZDI-24-1455: Linux Kernel Net Scheduler ATM Queuing Discipline Use-After-Free Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Tue, 05 Nov 2024

**ZDI-24-1454: Linux Kernel nftables Improper Validation of Array Index Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Tue, 05 Nov 2024

**ZDI-24-1453: X.Org Server XkbSetCompatMap Heap-based Buffer Overflow Privilege Escalation Vulnerability**

- [Link](#)

—

” “Mon, 04 Nov 2024

**ZDI-24-1452: Autodesk AutoCAD CATPART File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

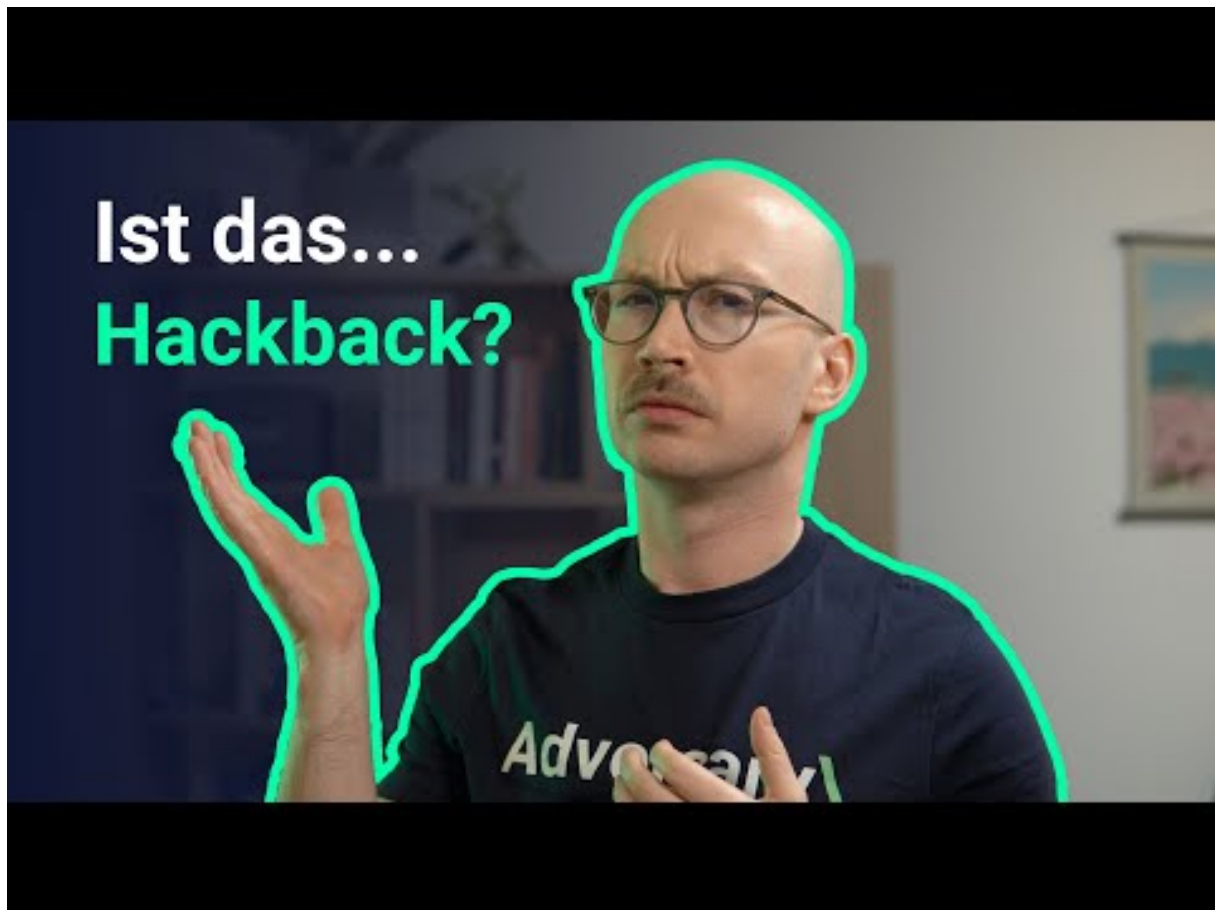
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Sophos spielt die UNO Reverse Karte ☒ (+ Redline Stealer)



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Nov)

Datum	Opfer	Land	Information
2024-11-04	Avis de Torino	[ITA]	<a href="#">Link</a>
2024-11-02	Memorial Hospital and Manor	[USA]	<a href="#">Link</a>
2024-11-02	Kumla kommun	[SWE]	<a href="#">Link</a>
2024-11-01	South East Technological University (SETU)	[IRL]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Nov)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-06	[LmayInteroute agency]	lynx	<a href="#">Link</a>
2024-11-05	[pacificglazing.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[nwhealthporter.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[wexfordcounty.org]	embargo	<a href="#">Link</a>
2024-11-05	[ebrso]	qilin	<a href="#">Link</a>
2024-11-05	[Model Die & Mold]	lynx	<a href="#">Link</a>
2024-11-04	[mh-m.org]	embargo	<a href="#">Link</a>
2024-11-05	[Falco Sult]	bianlian	<a href="#">Link</a>
2024-11-05	[apoyoconsultoria.com]	ransomhub	<a href="#">Link</a>
2024-11-05	[Webb Institute]	incransom	<a href="#">Link</a>
2024-11-05	[Fylde Coast Academy Trust]	rhysida	<a href="#">Link</a>
2024-11-04	[sundt.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[Memorial Hospital & Manor]	embargo	<a href="#">Link</a>
2024-11-02	[Scolari]	dragonforce	<a href="#">Link</a>
2024-11-05	[McMillan Electric Company]	medusa	<a href="#">Link</a>
2024-11-04	[maxdata.com.br]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-04	[goodline.com.au]	ransomhub	<a href="#">Link</a>
2024-11-04	[kenanasugarcompany.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[www.schweiker.de]	ransomhub	<a href="#">Link</a>
2024-11-04	[www.drbutlerandassociates.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[www.mssupply.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[fullfordelectric.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[College of Business - Tanzania]	hellcat	<a href="#">Link</a>
2024-11-04	[Ministry of Education - Jordan]	hellcat	<a href="#">Link</a>
2024-11-04	[Schneider Electric - France]	hellcat	<a href="#">Link</a>
2024-11-04	[International University of Sarajevo]	medusa	<a href="#">Link</a>
2024-11-04	[Whitaker Construction Group]	medusa	<a href="#">Link</a>
2024-11-04	[European External Action Service (EEAS)]	hunters	<a href="#">Link</a>
2024-11-04	[csucontracting.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[redphoenixconstruction.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[Air Specialists Heating & Air Conditioning]	hunters	<a href="#">Link</a>
2024-11-03	[krigerconstruction.com]	ransomhub	<a href="#">Link</a>
2024-11-03	[caseconstruction.com]	ransomhub	<a href="#">Link</a>
2024-11-03	[lambertstonecommercial.com]	ransomhub	<a href="#">Link</a>
2024-11-04	[Doctor 24x7]	killsec	<a href="#">Link</a>
2024-11-03	[Hemubo]	hunters	<a href="#">Link</a>
2024-11-03	[Elad municipality]	handala	<a href="#">Link</a>
2024-11-03	[Russell Law Firm, LLC]	bianlian	<a href="#">Link</a>
2024-11-03	[L & B Transport, L.L.C.]	bianlian	<a href="#">Link</a>
2024-11-03	[guardianhc]	stormous	<a href="#">Link</a>
2024-11-02	[bravodigitaltrader.co.uk]	ransomhub	<a href="#">Link</a>
2024-11-02	[SVP Worldwide]	blacksuit	<a href="#">Link</a>
2024-11-02	[Sumitomo]	killsec	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-11-01	[DieTech North America]	qilin	<a href="#">Link</a>
2024-11-01	[www.fatboysfleetandauto.com]	ransomhub	<a href="#">Link</a>
2024-11-01	[www.tigre.gob.ar]	ransomhub	<a href="#">Link</a>
2024-11-01	[www.usm.cl]	ransomhub	<a href="#">Link</a>
2024-11-01	[lighthouseelectric.com]	ransomhub	<a href="#">Link</a>
2024-11-01	[JS McCarthy Printers]	play	<a href="#">Link</a>
2024-11-01	[CGR Technologies]	play	<a href="#">Link</a>
2024-11-01	[lumiplan.com]	cactus	<a href="#">Link</a>
2024-11-01	[United Sleep Diagnostics]	medusa	<a href="#">Link</a>
2024-11-01	[eap.gr]	ransomhub	<a href="#">Link</a>
2024-11-01	[vikurverk.is]	lockbit3	<a href="#">Link</a>
2024-11-01	[mirandaproduce.com.ve]	lockbit3	<a href="#">Link</a>
2024-11-01	[Cerp Bretagne Nord]	hunters	<a href="#">Link</a>
2024-11-01	[Hope Valley Recovery]	rhysida	<a href="#">Link</a>
2024-11-01	[lsst.ac]	cactus	<a href="#">Link</a>
2024-11-01	[MCNA Dental]	everest	<a href="#">Link</a>
2024-11-01	[Arctrade]	everest	<a href="#">Link</a>

## 8 Quellen

### 8.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - [packetstormsecurity.com](https://packetstormsecurity.com)

- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>



## 9 Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

[info@cyberwald.com](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.