

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240703



## 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>17</b>
5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . .	17
<b>6 Cyberangriffe: (Jul)</b>	<b>18</b>
<b>7 Ransomware-Erpressungen: (Jul)</b>	<b>18</b>
<b>8 Quellen</b>	<b>19</b>
8.1 Quellenverzeichnis . . . . .	19
<b>9 Impressum</b>	<b>20</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

#### ***Android: Google schließt teils kritische Lücken am Juli-Patchday***

Google hat Updates für Android 12, 12L, 13 und 14 im Rahmen des Juli-Patchdays veröffentlicht. Sie schließen Rechteauserweiterungs-Lücken.

- [Link](#)

—

#### ***Update für IBM InfoSphere Information Server dichtet viele Sicherheitslücken ab***

IBM hat mehrere Sicherheitswarnungen zum InfoSphere Information Server herausgegeben. Aktualisierte Software korrigiert die Fehler.

- [Link](#)

—

#### ***Juniper: Notfall-Update für Junos OS auf SRX-Baureihe***

Juniper Networks schließt eine als hochriskant eingestufte DoS-Lücke im Juniper OS der SRX-Geräte mit einem Update außer der Reihe.

- [Link](#)

—

#### ***RegreSSHion: Sicherheitslücke in OpenSSH gibt geduldigen Angreifern Root-Rechte***

Wer die alte, neue Lücke im SSH-Server ausnutzen möchte, braucht Sitzfleisch: Bis zur Root-Shell dauert es 8 Stunden. Dafür klappt der Angriff aus der Ferne.

- [Link](#)

—

#### ***IP-Telefonie: Avaya IP Office stopft kritische Sicherheitslecks***

Updates für Avaya IP Office dichten Sicherheitslecks in der Software ab. Angreifer können dadurch Schadcode einschleusen.

- [Link](#)

—

#### ***Juniper: Kritische Lücke erlaubt Angreifern Übernahme von Session Smart Router***

Juniper Networks liefert außerplanmäßige Updates gegen eine kritische Sicherheitslücke in Session Smart Router, -Conductor und WAN Assurance Router.

- [Link](#)

—

#### ***APT-Angriff auf Fernwartungssoftware? Sicherheitsvorfall bei TeamViewer***

Noch ist über das Ausmaß des Angriffs gegen die Fernwartungssoftware nicht viel bekannt - erste Hinweise auf die Urheber deuten auf Profis hin.

- [Link](#)

---

**Bitte patchen! Security-Update behebt kritische Schwachstelle in GitLab**

Eine Reihe von Schwachstellen ermöglichen es in GitLab, CI-Pipelines als anderer User zu starten oder Cross-Site-Scripting über Commit Notes einzuschleusen.

- [Link](#)

---

**Google Quickshare: Sicherheitslücke ermöglicht ungefragtes Senden von Dateien**

Googles Quickshare, auch als Nearby Share bekannt, kann Angreifern ungefragt Daten an Windows-Rechner schicken lassen.

- [Link](#)

---

**JavaScript-Service Polyfill.io: 100.000 Sites binden Schadcode über CDN ein**

Mehrere Sicherheitsforscher melden eine aktive Bedrohung durch das Content Delivery Network von Polyfill.io. Google sperrt Werbung von betroffenen Ads-Seiten.

- [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	0.960230000	0.994980000	<a href="#">Link</a>
CVE-2023-6895	0.920390000	0.989590000	<a href="#">Link</a>
CVE-2023-6553	0.934680000	0.991130000	<a href="#">Link</a>
CVE-2023-5360	0.911260000	0.988860000	<a href="#">Link</a>
CVE-2023-52251	0.920390000	0.989600000	<a href="#">Link</a>
CVE-2023-4966	0.971290000	0.998070000	<a href="#">Link</a>
CVE-2023-49103	0.938900000	0.991630000	<a href="#">Link</a>
CVE-2023-48795	0.962520000	0.995440000	<a href="#">Link</a>
CVE-2023-47246	0.953220000	0.993740000	<a href="#">Link</a>
CVE-2023-46805	0.958670000	0.994670000	<a href="#">Link</a>
CVE-2023-46747	0.972100000	0.998360000	<a href="#">Link</a>
CVE-2023-46604	0.963890000	0.995790000	<a href="#">Link</a>
CVE-2023-4542	0.924200000	0.990010000	<a href="#">Link</a>
CVE-2023-43208	0.956050000	0.994250000	<a href="#">Link</a>
CVE-2023-43177	0.959300000	0.994810000	<a href="#">Link</a>
CVE-2023-42793	0.970430000	0.997700000	<a href="#">Link</a>
CVE-2023-41265	0.920320000	0.989580000	<a href="#">Link</a>
CVE-2023-39143	0.944760000	0.992370000	<a href="#">Link</a>
CVE-2023-38646	0.906240000	0.988520000	<a href="#">Link</a>
CVE-2023-38205	0.954590000	0.993980000	<a href="#">Link</a>
CVE-2023-38203	0.968820000	0.997200000	<a href="#">Link</a>
CVE-2023-38146	0.905210000	0.988440000	<a href="#">Link</a>
CVE-2023-38035	0.974610000	0.999600000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.965980000	0.996350000	<a href="#">Link</a>
CVE-2023-3519	0.965360000	0.996190000	<a href="#">Link</a>
CVE-2023-35082	0.967870000	0.996920000	<a href="#">Link</a>
CVE-2023-35078	0.968330000	0.997080000	<a href="#">Link</a>
CVE-2023-34993	0.971260000	0.998060000	<a href="#">Link</a>
CVE-2023-34960	0.927460000	0.990320000	<a href="#">Link</a>
CVE-2023-34634	0.927960000	0.990360000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988540000	<a href="#">Link</a>
CVE-2023-34362	0.969370000	0.997350000	<a href="#">Link</a>
CVE-2023-34039	0.945410000	0.992480000	<a href="#">Link</a>
CVE-2023-3368	0.933870000	0.991050000	<a href="#">Link</a>
CVE-2023-33246	0.972570000	0.998560000	<a href="#">Link</a>
CVE-2023-32315	0.973600000	0.999060000	<a href="#">Link</a>
CVE-2023-30625	0.938290000	0.991530000	<a href="#">Link</a>
CVE-2023-30013	0.962250000	0.995360000	<a href="#">Link</a>
CVE-2023-29300	0.969840000	0.997520000	<a href="#">Link</a>
CVE-2023-29298	0.943950000	0.992230000	<a href="#">Link</a>
CVE-2023-28771	0.918640000	0.989440000	<a href="#">Link</a>
CVE-2023-28343	0.948520000	0.992970000	<a href="#">Link</a>
CVE-2023-28121	0.923740000	0.989920000	<a href="#">Link</a>
CVE-2023-27524	0.970400000	0.997680000	<a href="#">Link</a>
CVE-2023-27372	0.973020000	0.998770000	<a href="#">Link</a>
CVE-2023-27350	0.969800000	0.997500000	<a href="#">Link</a>
CVE-2023-26469	0.932230000	0.990880000	<a href="#">Link</a>
CVE-2023-26360	0.957000000	0.994410000	<a href="#">Link</a>
CVE-2023-26035	0.967100000	0.996670000	<a href="#">Link</a>
CVE-2023-25717	0.956860000	0.994380000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.970160000	0.997610000	<a href="#">Link</a>
CVE-2023-2479	0.963760000	0.995760000	<a href="#">Link</a>
CVE-2023-24489	0.973550000	0.999030000	<a href="#">Link</a>
CVE-2023-23752	0.954250000	0.993930000	<a href="#">Link</a>
CVE-2023-23397	0.901800000	0.988250000	<a href="#">Link</a>
CVE-2023-23333	0.963260000	0.995630000	<a href="#">Link</a>
CVE-2023-22527	0.970550000	0.997740000	<a href="#">Link</a>
CVE-2023-22518	0.965950000	0.996340000	<a href="#">Link</a>
CVE-2023-22515	0.973330000	0.998930000	<a href="#">Link</a>
CVE-2023-21839	0.956220000	0.994300000	<a href="#">Link</a>
CVE-2023-21554	0.950840000	0.993310000	<a href="#">Link</a>
CVE-2023-20887	0.971080000	0.997970000	<a href="#">Link</a>
CVE-2023-1671	0.964510000	0.995910000	<a href="#">Link</a>
CVE-2023-0669	0.971300000	0.998070000	<a href="#">Link</a>

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

Tue, 02 Jul 2024

#### **[NEU] [hoch] Samsung Android: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Samsung Android ausnutzen, um seine Privilegien zu erweitern, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

Tue, 02 Jul 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, 02 Jul 2024

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

Ein entfernter, anonymer 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](#)

—

Tue, 02 Jul 2024

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

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

- [Link](#)

—

Tue, 02 Jul 2024

**[NEU] [hoch] Spotfire Analytics: Mehrere Schwachstellen**

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Spotfire Analytics, Spotfire Server und Spotfire Statistics Services ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Tue, 02 Jul 2024

**[NEU] [hoch] Splunk Enterprise: Mehrere Schwachstellen**

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Splunk Enterprise ausnutzen, um beliebigen Programmcode auszuführen, einen Cross-Site-Scripting-Angriff durchzuführen, mehrere Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren und vertrauliche Informationen preiszugeben

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen**

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um einen Denial-of-Service-Zustand auslösen, Informationen offenzulegen, Daten zu manipulieren, Sicherheitsmaßnahmen zu umgehen oder einen Cross-Site-Scripting-Angriff durchführen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen**

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um beliebigen Code auszuführen, einen 'Denial of Service'-Zustand zu verursachen, seine Privilegien zu erweitern und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Red Hat Quarkus: Schwachstelle ermöglicht die Umgehung von Sicherheitsmaßnahmen oder die Verursachung eines Denial-of-Service-Zustands**

Ein entfernter anonymer Angreifer kann eine Schwachstelle in Red Hat Quarkus ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 02 Jul 2024

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

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um Informationen offenzulegen, beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service**

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

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Splunk Enterprise ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder unbekannte Auswirkungen zu verursachen.

- [Link](#)

—

Tue, 02 Jul 2024

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

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

- [Link](#)

—

Tue, 02 Jul 2024

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

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

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren, Phishing-Angriffe durchzuführen oder Cross-Site Scripting (XSS)-Angriffe auszuführen. Einige dieser Schwachstellen erfordern eine Benutzerinteraktion, um sie erfolgreich auszunutzen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Dateien zu manipulieren oder Informationen offenzulegen.

- [Link](#)

—

Tue, 02 Jul 2024

**[UPDATE] [hoch] VMware Tanzu Spring Framework: Schwachstelle ermöglicht Manipulation von Daten**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Framework ausnutzen, um Daten zu manipulieren oder Informationen offenzulegen.

- [Link](#)

Tue, 02 Jul 2024

**[UPDATE] [hoch] LibreOffice: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

**3.3 Sicherheitslücken Meldungen von Tenable**

Datum	Schwachstelle	Bewertung
7/2/2024	[CBL Mariner 2.0 Security Update: php (CVE-2024-1874)]	critical
7/2/2024	[CBL Mariner 2.0 Security Update: unzip (CVE-2008-0888)]	critical
7/2/2024	[CBL Mariner 2.0 Security Update: zip (CVE-2018-13410)]	critical
7/2/2024	[RHEL 8 : less (RHSA-2024:4256)]	critical
7/2/2024	[RHEL 8 : go-toolset (RHSA-2024:4237)]	critical
7/2/2024	[CBL Mariner 2.0 Security Update: vte291 (CVE-2024-37535)]	high
7/2/2024	[CBL Mariner 2.0 Security Update: nodejs18 / nodejs / libuv (CVE-2024-22017)]	high
7/2/2024	[CBL Mariner 2.0 Security Update: libdb (CVE-2017-3611)]	high
7/2/2024	[CBL Mariner 2.0 Security Update: unzip (CVE-2014-9636)]	high
7/2/2024	[CBL Mariner 2.0 Security Update: libdb (CVE-2017-3605)]	high
7/2/2024	[CBL Mariner 2.0 Security Update: libdb (CVE-2017-3617)]	high
7/2/2024	[CBL Mariner 2.0 Security Update: git (CVE-2024-32465)]	high

Datum	Schwachstelle	Bewertung
7/2/2024	[CBL Mariner 2.0 Security Update: patch (CVE-2018-6952)]	high
7/2/2024	[RHEL 8 : libreoffice (RHSA-2024:4242)]	high
7/2/2024	[RHEL 8 : Red Hat OpenStack Platform 16.2.6 (RHSA-2024:4273)]	high
7/2/2024	[RHEL 9 : Red Hat OpenStack Platform 17.1.3 (RHSA-2024:4272)]	high
7/2/2024	[RHEL 9 : qemu-kvm (RHSA-2024:4276)]	high
7/2/2024	[RHEL 8 : 389-ds (RHSA-2024:4235)]	high
7/2/2024	[RHEL 9 : qemu-kvm (RHSA-2024:4278)]	high
7/2/2024	[RHEL 8 : Red Hat OpenStack Platform 17.1.3 (openstack-nova) (RHSA-2024:4274)]	high
7/2/2024	[RHEL 7 : pki-core (RHSA-2024:4222)]	high
7/2/2024	[RHEL 8 : libuv (RHSA-2024:4247)]	high
7/2/2024	[RHEL 9 : qemu-kvm (RHSA-2024:4277)]	high
7/2/2024	[RHEL 8 : openldap (RHSA-2024:4264)]	high
7/2/2024	[RHEL 8 : xmlrpc-c (RHSA-2024:4259)]	high
7/2/2024	[Oracle Linux 7 : pki-core (ELSA-2024-4222)]	high
7/2/2024	[Fedora 40 : openssh (2024-dc89a2e1bf)]	high
7/2/2024	[Fedora 39 : openssh (2024-213f33544e)]	high
7/2/2024	[Slackware Linux 15.0 / current httpd Multiple Vulnerabilities (SSA:2024-184-01)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Tue, 02 Jul 2024

#### **WordPress FooGallery 2.4.16 Cross Site Scripting**

WordPress FooGallery plugin version 2.4.16 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—  
" "Tue, 02 Jul 2024

**WordPress Gallery 2.3.6 Cross Site Scripting**

WordPress Gallery version 2.3.6 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

" "Tue, 02 Jul 2024

**PowerVR Driver Missing Sanitization**

The PowerVR driver does not sanitize ZS-Buffer / MSAA scratch firmware addresses.

- [Link](#)

—

" "Mon, 01 Jul 2024

**Packet Storm New Exploits For June, 2024**

This archive contains all of the 65 exploits added to Packet Storm in June, 2024.

- [Link](#)

—

" "Mon, 01 Jul 2024

**OpenSSH Server regreSSHion Remote Code Execution**

Qualys has discovered a a signal handler race condition vulnerability in OpenSSH's server, sshd. If a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then sshd's SIGALRM handler is called asynchronously, but this signal handler calls various functions that are not async-signal-safe - for example, syslog(). This race condition affects sshd in its default configuration.

- [Link](#)

—

" "Mon, 01 Jul 2024

**Simple Laboratory Management System 1.0 SQL Injection**

Simple Laboratory Management System version 1.0 suffers from a remote time-based SQL injection vulnerability.

- [Link](#)

—

" "Mon, 01 Jul 2024

**Azon Dominator Affiliate Marketing Script SQL Injection**

Azon Dominator Affiliate Marketing Script suffers from a remote SQL injection vulnerability.

- [Link](#)

—

" "Mon, 01 Jul 2024

**WordPress WPCode Lite 2.1.14 Cross Site Scripting**

WordPress WPCode Lite plugin version 2.1.14 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 01 Jul 2024

***Xhibiter NFT Marketplace 1.10.2 SQL Injection***

Xhibiter NFT Marketplace version 1.10.2 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 01 Jul 2024

***Customer Support System 1.0 Cross Site Scripting***

Customer Support System version 1.0 suffers from a persistent cross site scripting vulnerability. Original discovery of cross site scripting in this version is attributed to Ahmed Abba in November of 2020.

- [Link](#)

—

” “Thu, 27 Jun 2024

***SimpCMS 0.1 Cross Site Scripting***

SimpCMS version 0.1 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

***Ollama Remote Code Execution***

Ollama versions prior to 0.1.34 suffer from a remote code execution vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

***SolarWinds Platform 2024.1 SR1 Race Condition***

SolarWinds Platform version 2024.1 SR1 suffers from a race condition vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

***Automad 2.0.0-alpha.4 Cross Site Scripting***

Automad version 2.0.0-alpha.4 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Wed, 26 Jun 2024

***Poultry Farm Management System 1.0 Shell Upload***

Poultry Farm Management System version 1.0 remote shell upload exploit. This is a variant of the ori-

ginal discovery of this flaw in this software version by Hejap Zairy in March of 2022.

- [Link](#)

—

” “Tue, 25 Jun 2024

***Faronics WINSelect Hardcoded Credentials / Bad Permissions / Unhashed Password***

Faronics WINSelect versions prior to 8.30.xx.903 suffer from having hardcoded credentials, storing unhashed passwords, and configuration file modification vulnerabilities.

- [Link](#)

—

” “Mon, 24 Jun 2024

***Netis MW5360 Remote Command Execution***

The Netis MW5360 router has a command injection vulnerability via the password parameter on the login page. The vulnerability stems from improper handling of the ”password” parameter within the router’s web interface. The router’s login page authorization can be bypassed by simply deleting the authorization header, leading to the vulnerability. All router firmware versions up to V1.0.1.3442 are vulnerable. Attackers can inject a command in the password parameter, encoded in base64, to exploit the command injection vulnerability. When exploited, this can lead to unauthorized command execution, potentially allowing the attacker to take control of the router.

- [Link](#)

—

” “Mon, 24 Jun 2024

***Edu-Sharing Arbitrary File Upload***

Edu-Sharing suffers from an arbitrary file upload vulnerability. Versions below 8.0.8-RC2, 8.1.4-RC0, and 9.0.0-RC19 are affected.

- [Link](#)

—

” “Mon, 24 Jun 2024

***Flatboard 3.2 Cross Site Scripting***

Flatboard version 3.2 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 24 Jun 2024

***Carbon Forum 5.9.0 Cross Site Request Forgery / SQL Injection***

Carbon Forum version 5.9.0 suffers from access control, cross site request forgery, file upload, outdated library, and remote SQL injection vulnerabilities.

- [Link](#)

—

” “Mon, 24 Jun 2024



**Student Attendance Management System 1.0 SQL Injection**

Student Attendance Management System version 1.0 suffers from a remote SQL Injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 24 Jun 2024

**Paradox IP150 Internet Module 1.40.00 Cross Site Request Forgery**

Paradox IP150 Internet Module version 1.40.00 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Thu, 20 Jun 2024

**TURPENTINE XNU Kernel Buffer Overflow**

CVE-2024-27815 is a buffer overflow in the XNU kernel that was reported in sbconcat\_mbufs. It was publicly fixed in xnu-10063.121.3, released with macOS 14.5, iOS 17.5, and visionOS 1.2. This bug was introduced in xnu-10002.1.13 (macOS 14.0/ iOS 17.0) and was fixed in xnu-10063.121.3 (macOS 14.5/ iOS 17.5). The bug affects kernels compiled with CONFIG\_MBUF\_MCACHE.

- [Link](#)

—

” “Wed, 19 Jun 2024

**Bagisto 2.1.2 Client-Side Template Injection**

Bagisto version 2.1.2 suffers from a client-side template injection vulnerability.

- [Link](#)

—

” “Wed, 19 Jun 2024

**User Registration And Management System 3.2 SQL Injection**

User Registration and Management System version 3.2 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

”

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

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
-------	-------	------	-------------

## 7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-02	[merrymanhouse.org]	lockbit3	<a href="#">Link</a>
2024-07-02	[fairfieldmemorial.org]	lockbit3	<a href="#">Link</a>
2024-07-02	[www.daesangamerica.com]	ransomhub	<a href="#">Link</a>
2024-07-02	[P1 Technologies]	akira	<a href="#">Link</a>
2024-07-02	[Conexus Medstaff]	akira	<a href="#">Link</a>
2024-07-02	[Salton]	akira	<a href="#">Link</a>
2024-07-01	[www.sfmedical.de]	ransomhub	<a href="#">Link</a>
2024-07-02	[WheelerShip]	hunters	<a href="#">Link</a>
2024-07-02	[Grand Rapids Gravel]	dragonforce	<a href="#">Link</a>
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	<a href="#">Link</a>
2024-07-02	[Elite Fitness]	dragonforce	<a href="#">Link</a>
2024-07-02	[Gray & Adams]	dragonforce	<a href="#">Link</a>
2024-07-02	[Vermont Panurgy]	dragonforce	<a href="#">Link</a>
2024-07-01	[floridahealth.gov]	ransomhub	<a href="#">Link</a>
2024-07-01	[www.nttdata.ro]	ransomhub	<a href="#">Link</a>
2024-07-01	[Super Gardens]	dragonforce	<a href="#">Link</a>
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	<a href="#">Link</a>
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	<a href="#">Link</a>
2024-07-01	[SYNERGY PEANUT]	akira	<a href="#">Link</a>
2024-07-01	[Ethypharm]	underground	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-01	[latiusa.co.id]	lockbit3	<a href="#">Link</a>
2024-07-01	[kbc-zagreb.hr]	lockbit3	<a href="#">Link</a>
2024-07-01	[maxcess-logistics.com]	killsec	<a href="#">Link</a>
2024-07-01	[Independent Education System]	handala	<a href="#">Link</a>
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	<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.