

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240714



## 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>23</b>
8.1 Quellenverzeichnis . . . . .	23
<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

#### ***Sicherheitslücken GitLab: Angreifer können Softwareentwicklung manipulieren***

GitLab Community Edition und Enterprise Edition sind verwundbar. Die Entwickler raten zu einem zügigen Update.

- [Link](#)

—

#### ***Webkonferenzen: Zoom dichtet acht Sicherheitslücken ab***

In der Webkonferenz-Software klaffen mehrere Sicherheitslücken, eine davon hochriskant. Updates dichten sie ab.

- [Link](#)

—

#### ***Nvidia: Angreifer können Schadcode durch Grafikkartentreiber-Lücke schieben***

Es sind Attacken auf Windows-PCs mit unter anderem GeForce- oder RTX-Grafikkarten möglich. Berichte zu Angriffen gibt es aber noch nicht.

- [Link](#)

—

#### ***Cisco: Secure Boot bei einigen Routern umgehbar, Anfälligkeit auf RADIUS-Lücke***

Angreifer können einigen Cisco-Routern manipulierte Software unterschieben. Die Entwickler prüfen, welche Geräte von der RADIUS-Lücke betroffen sind.

- [Link](#)

—

#### ***Juniper Networks: 46 Sicherheitswarnungen veröffentlicht***

Juniper Networks hat zu seinem regulären Update-Tag 46 Sicherheitsmitteilungen veröffentlicht. Admins sollten die Updates zügig installieren.

- [Link](#)

—

#### ***VMware stopft SQL-Injection-Lücke in Aria Automation***

Angreifer können eine Schwachstelle in VMware Aria Automation missbrauchen, um eigene Befehle mittels SQL-Injection einzuschleusen. Updates stehen bereit.

- [Link](#)

—

#### ***Blast-RADIUS: Sicherheitslücke im Netzwerkprotokoll RADIUS veröffentlicht***

Lange bekannte Schwachstellen können dem RADIUS-Protokoll zum Verhängnis werden, das vor allem im Enterprise-Umfeld in sehr vielen Netzwerken eingesetzt wird.

- [Link](#)

---

**Patchday Fortinet: FortiAI Ops und FortiOS gegen mögliche Attacken gerüstet**

Angriffe können mehrere Produkte von Fortinet ins Visier nehmen und unter anderem sensible Daten einsehen.

- [Link](#)

---

**OpenSSH: Weitere RegreSSHion-artige Lücke entdeckt**

Die RegreSSHion-Lücke ermöglichte Angreifern Root-Zugriff. Ein IT-Forscher hat eine weitere ähnliche Lücke in OpenSSH von RHEL 9 und Abkömmlingen entdeckt.

- [Link](#)

---

**Citrix stopft teils kritische Sicherheitslücken in mehreren Produkten**

Citrix hat Sicherheitswarnungen zu mehreren Produkten veröffentlicht. Updates schließen teils kritische Schwachstellen darin.

- [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	0.962510000	0.995510000	<a href="#">Link</a>
CVE-2023-6895	0.922010000	0.989830000	<a href="#">Link</a>
CVE-2023-6553	0.936860000	0.991410000	<a href="#">Link</a>
CVE-2023-5360	0.911260000	0.988990000	<a href="#">Link</a>
CVE-2023-52251	0.930900000	0.990770000	<a href="#">Link</a>
CVE-2023-4966	0.971290000	0.998140000	<a href="#">Link</a>
CVE-2023-49103	0.953130000	0.993800000	<a href="#">Link</a>
CVE-2023-48795	0.965740000	0.996390000	<a href="#">Link</a>
CVE-2023-47246	0.951210000	0.993440000	<a href="#">Link</a>
CVE-2023-46805	0.958670000	0.994740000	<a href="#">Link</a>
CVE-2023-46747	0.972630000	0.998620000	<a href="#">Link</a>
CVE-2023-46604	0.963510000	0.995770000	<a href="#">Link</a>
CVE-2023-4542	0.924200000	0.990090000	<a href="#">Link</a>
CVE-2023-43208	0.959520000	0.994920000	<a href="#">Link</a>
CVE-2023-43177	0.962660000	0.995550000	<a href="#">Link</a>
CVE-2023-42793	0.970470000	0.997790000	<a href="#">Link</a>
CVE-2023-41265	0.905890000	0.988610000	<a href="#">Link</a>
CVE-2023-39143	0.940070000	0.991790000	<a href="#">Link</a>
CVE-2023-38646	0.906240000	0.988660000	<a href="#">Link</a>
CVE-2023-38205	0.954590000	0.994090000	<a href="#">Link</a>
CVE-2023-38203	0.968820000	0.997270000	<a href="#">Link</a>
CVE-2023-38146	0.905210000	0.988570000	<a href="#">Link</a>
CVE-2023-38035	0.974190000	0.999410000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.963940000	0.995870000	<a href="#">Link</a>
CVE-2023-3519	0.965360000	0.996280000	<a href="#">Link</a>
CVE-2023-35082	0.967060000	0.996750000	<a href="#">Link</a>
CVE-2023-35078	0.968330000	0.997140000	<a href="#">Link</a>
CVE-2023-34993	0.972880000	0.998730000	<a href="#">Link</a>
CVE-2023-34960	0.929370000	0.990620000	<a href="#">Link</a>
CVE-2023-34634	0.927960000	0.990410000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988680000	<a href="#">Link</a>
CVE-2023-34362	0.969920000	0.997630000	<a href="#">Link</a>
CVE-2023-34039	0.944490000	0.992380000	<a href="#">Link</a>
CVE-2023-3368	0.933870000	0.991100000	<a href="#">Link</a>
CVE-2023-33246	0.972790000	0.998690000	<a href="#">Link</a>
CVE-2023-32315	0.973570000	0.999070000	<a href="#">Link</a>
CVE-2023-30625	0.943100000	0.992160000	<a href="#">Link</a>
CVE-2023-30013	0.962250000	0.995440000	<a href="#">Link</a>
CVE-2023-29300	0.968380000	0.997160000	<a href="#">Link</a>
CVE-2023-29298	0.943170000	0.992180000	<a href="#">Link</a>
CVE-2023-28771	0.902140000	0.988390000	<a href="#">Link</a>
CVE-2023-28343	0.948520000	0.993000000	<a href="#">Link</a>
CVE-2023-28121	0.909760000	0.988870000	<a href="#">Link</a>
CVE-2023-27524	0.970570000	0.997830000	<a href="#">Link</a>
CVE-2023-27372	0.973020000	0.998800000	<a href="#">Link</a>
CVE-2023-27350	0.970130000	0.997670000	<a href="#">Link</a>
CVE-2023-26469	0.935230000	0.991240000	<a href="#">Link</a>
CVE-2023-26360	0.962310000	0.995470000	<a href="#">Link</a>
CVE-2023-26035	0.967100000	0.996760000	<a href="#">Link</a>
CVE-2023-25717	0.956860000	0.994460000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-25194	0.969960000	0.997640000	<a href="#">Link</a>
CVE-2023-2479	0.963740000	0.995820000	<a href="#">Link</a>
CVE-2023-24489	0.973310000	0.998940000	<a href="#">Link</a>
CVE-2023-23752	0.954250000	0.994030000	<a href="#">Link</a>
CVE-2023-23397	0.901800000	0.988370000	<a href="#">Link</a>
CVE-2023-23333	0.964220000	0.995920000	<a href="#">Link</a>
CVE-2023-22527	0.970550000	0.997820000	<a href="#">Link</a>
CVE-2023-22518	0.965070000	0.996180000	<a href="#">Link</a>
CVE-2023-22515	0.973330000	0.998960000	<a href="#">Link</a>
CVE-2023-21839	0.957210000	0.994530000	<a href="#">Link</a>
CVE-2023-21554	0.950840000	0.993360000	<a href="#">Link</a>
CVE-2023-20887	0.970320000	0.997760000	<a href="#">Link</a>
CVE-2023-1671	0.962480000	0.995510000	<a href="#">Link</a>
CVE-2023-0669	0.969330000	0.997420000	<a href="#">Link</a>

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

Fri, 12 Jul 2024

#### **[UPDATE] [hoch] Apache HttpComponents: Schwachstelle ermöglicht Täuschung des Nutzers**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache HttpComponents ausnutzen, um den Nutzer zu täuschen.

- [Link](#)

—

Fri, 12 Jul 2024

#### **[UPDATE] [hoch] Drupal: Mehrere Schwachstellen**

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Drupal ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Daten zu manipulieren, um einen Denial of Service Zustand herbeizuführen und um beliebigen Code auszuführen.

- [Link](#)



—

Fri, 12 Jul 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](#)

—

Fri, 12 Jul 2024

**[NEU] [hoch] Fabasoft Folio: Schwachstelle ermöglicht Codeausführung**

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in Fabasoft Folio ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 12 Jul 2024

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

Ein entfernter, anonym Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programmcode mit root Rechten auszuführen.

- [Link](#)

—

Fri, 12 Jul 2024

**[UPDATE] [hoch] Python: Schwachstelle ermöglicht Manipulation**

Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um HTTP Anfragen zu manipulieren.

- [Link](#)

—

Fri, 12 Jul 2024

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Python ausnutzen, um Dateien zu manipulieren und Schutzmechanismen zu umgehen.

- [Link](#)

—

Fri, 12 Jul 2024

**[UPDATE] [hoch] Python: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Python ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen oder Informationen offenzulegen.

- [Link](#)

—

Fri, 12 Jul 2024

**[UPDATE] [hoch] Python: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit**

**Benutzerrechten**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen.

- [Link](#)

—

Fri, 12 Jul 2024

**[UPDATE] [kritisch] Python: Schwachstelle ermöglicht Codeausführung**

Ein Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 12 Jul 2024

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

Ein lokaler Angreifer kann eine Schwachstelle in Python ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 12 Jul 2024

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

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

- [Link](#)

—

Fri, 12 Jul 2024

**[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen ermöglichen HTTP Response Splitting**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um einen Response Splitting Angriff durchzuführen.

- [Link](#)

—

Fri, 12 Jul 2024

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

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 12 Jul 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Komponente libvpx ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

---

Fri, 12 Jul 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

---

Fri, 12 Jul 2024

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

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.

- [Link](#)

---

Fri, 12 Jul 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren, Cross-Site Scripting (XSS)-Angriffe durchzuführen oder einen Men-in-the-Middle-Angriff auszuführen.

- [Link](#)

---

Fri, 12 Jul 2024

**[UPDATE] [hoch] Fluent Bit: Schwachstelle ermöglicht Codeausführung, Offenlegung von Informationen und DoS**

Ein entfernter anonymer Angreifer kann eine Schwachstelle in Fluent Bit ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

---

Fri, 12 Jul 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder

Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2023-52802)]	critical
7/12/2024	[RHEL 8 : pcs (Unpatched Vulnerability)]	critical
7/12/2024	[RHEL 9 : pcs (Unpatched Vulnerability)]	critical
7/13/2024	[Fedora 39 : pgadmin4 (2024-9820d9491f)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 10 for SLE 15 SP5) (SUSE-SU-2024:2446-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 12 for SLE 15 SP5) (SUSE-SU-2024:2473-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 24 for SLE 15 SP4) (SUSE-SU-2024:2447-1)]	high
7/13/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2024:2415-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 13 for SLE 15 SP4) (SUSE-SU-2024:2437-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 25 for SLE 15 SP4) (SUSE-SU-2024:2448-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 13 for SLE 15 SP5) (SUSE-SU-2024:2474-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 11 for SLE 15 SP5) (SUSE-SU-2024:2472-1)]	high
7/13/2024	[SUSE SLES15 Security Update : kernel (Live Patch 26 for SLE 15 SP4) (SUSE-SU-2024:2449-1)]	high

Datum	Schwachstelle	Bewertung
7/13/2024	[FreeBSD : electron29 – multiple vulnerabilities (55d4a92f-c75f-43e8-ab1f-4a0efc9795c4)]	high
7/13/2024	[FreeBSD : electron30 – multiple vulnerabilities (6410f91d-1214-4f92-b7e0-852e39e265f9)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: glibc (CVE-2024-33602)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: glibc (CVE-2024-33601)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: apparmor (CVE-2024-31755)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-39291)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-26933)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-38664)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-36477)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: vim (CVE-2023-5535)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: pytorch (CVE-2024-31583)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2021-3847)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2023-6817)]	high
7/13/2024	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-26913)]	high
7/12/2024	[RHEL 7 : qemu-kvm (Unpatched Vulnerability)]	high
7/12/2024	[RHEL 9 : ghostscript (Unpatched Vulnerability)]	high
7/12/2024	[RHEL 8 : qemu-kvm (Unpatched Vulnerability)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Thu, 11 Jul 2024

#### **Atlassian Confluence Administrator Code Macro Remote Code Execution**

This Metasploit module exploits an authenticated administrator-level vulnerability in Atlassian Confluence, tracked as CVE-2024-21683. The vulnerability exists due to the Rhino script engine parser evaluating tainted data from uploaded text files. This facilitates arbitrary code execution. This exploit will

authenticate, validate user privileges, extract the underlying host OS information, then trigger remote code execution. All versions of Confluence prior to 7.17 are affected, as are many versions up to 8.9.0.

- [Link](#)

—

” “Thu, 11 Jul 2024

***LumisXP 16.1.x Cross Site Scripting***

LumisXP versions 15.0.x through 16.1.x suffer from a cross site scripting vulnerability in XsltResultControllerHtml.jsp.

- [Link](#)

—

” “Thu, 11 Jul 2024

***LumisXP 16.1.x Cross Site Scripting***

LumisXP versions 15.0.x through 16.1.x suffer from a cross site scripting vulnerability in UrlAccessibilityEvaluation.jsp.

- [Link](#)

—

” “Thu, 11 Jul 2024

***LumisXP 16.1.x Cross Site Scripting***

LumisXP versions 15.0.x through 16.1.x suffer from a cross site scripting vulnerability in main.jsp

- [Link](#)

—

” “Thu, 11 Jul 2024

***LumisXP 16.1.x Hardcoded Credentials / IDOR***

LumisXP versions 15.0.x through 16.1.x have a hardcoded privileged identifier that allows attackers to bypass authentication and access internal pages and other sensitive information.

- [Link](#)

—

” “Thu, 11 Jul 2024

***WordPress Poll Maker 5.3.2 SQL Injection***

WordPress Poll Maker plugin version 5.3.2 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Thu, 11 Jul 2024

***ESET NOD32 Antivirus 17.2.7.0 Unquoted Service Path***

ESET NOD32 Antivirus version 17.2.7.0 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Wed, 10 Jul 2024

**Microsoft SharePoint Remote Code Execution**

This archive contains three proof of concepts exploit for multiple Microsoft SharePoint remote code execution vulnerabilities.

- [Link](#)

—

” “Tue, 09 Jul 2024

**Ivanti EPM RecordGoodApp SQL Injection / Remote Code Execution**

Ivanti Endpoint Manager (EPM) 2022 SU5 and prior versions are susceptible to an unauthenticated SQL injection vulnerability which can be leveraged to achieve unauthenticated remote code execution.

- [Link](#)

—

” “Mon, 08 Jul 2024

**WordPress Poll 2.3.6 SQL Injection**

WordPress Poll plugin version 2.3.6 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 08 Jul 2024

**VMWare Aria Operations For Networks Command Injection**

VMWare Aria Operations for Networks (vRealize Network Insight) is vulnerable to command injection when accepting user input through the Apache Thrift RPC interface. This is a proof of concept exploit.

- [Link](#)

—

” “Mon, 08 Jul 2024

**Veeam Backup Enterprise Manager Authentication Bypass**

Veeam Backup Enterprise Manager authentication bypass proof of concept exploit. Versions prior to 12.1.2.172 are vulnerable.

- [Link](#)

—

” “Mon, 08 Jul 2024

**Veeam Recovery Orchestrator Authentication Bypass**

Veeam Recovery Orchestrator authentication bypass proof of concept exploit.

- [Link](#)

—

” “Mon, 08 Jul 2024

**Telerik Report Server Deserialization / Authentication Bypass**

Telerik Report Server deserialization and authentication bypass exploit chain that makes use of the vulnerabilities noted in CVE-2024-4358 and CVE-2024-1800.

- [Link](#)

—

” “Mon, 08 Jul 2024

***Progress WhatsUp Gold WriteDatafile Unauthenticated Remote Code Execution***

Progress WhatsUp Gold WriteDatafile unauthenticated remote code execution proof of concept exploit.

- [Link](#)

—

” “Mon, 08 Jul 2024

***Progress WhatsUp Gold GetFileWithoutZip Unauthenticated Remote Code Execution***

Progress WhatsUp Gold GetFileWithoutZip unauthenticated remote code execution proof of concept exploit.

- [Link](#)

—

” “Mon, 08 Jul 2024

***Progress WhatsUp Gold SetAdminPassword Privilege Escalation***

Progress WhatsUp Gold SetAdminPassword local privilege escalation proof of concept exploit.

- [Link](#)

—

” “Mon, 08 Jul 2024

***ResidenceCMS 2.10.1 Cross Site Scripting***

ResidenceCMS versions 2.10.1 and below suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 08 Jul 2024

***PMS 2024 1.0 SQL Injection***

PMS 2024 version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 08 Jul 2024

***Simple Online Banking System 1.0 SQL Injection***

Simple Online Banking System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 08 Jul 2024

***Microsoft Office 365 Remote Code Execution***

Microsoft Office 365 appears susceptible to macro code execution that can result in remote code exe-



cution.

- [Link](#)

—

” “Fri, 05 Jul 2024

**WordPress Video Gallery - YouTube Gallery And Vimeo Gallery 2.3.6 SQL Injection**

WordPress Video Gallery - YouTube Gallery And Vimeo Gallery version 2.3.6 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Fri, 05 Jul 2024

**Cinema Booking System 1.0 SQL Injection / Cross Site Request Forgery**

Cinema Booking System version 1.0 suffers from remote SQL injection and cross site request forgery vulnerabilities.

- [Link](#)

—

” “Thu, 04 Jul 2024

**Helmholz Industrial Router REX100 / MBConnectline mbNET.mini 2.2.11 Command Injection**

Helmholz Industrial Router REX100 and MBConnectline mbNET.mini versions 2.2.11 and below suffer from a command injection vulnerability.

- [Link](#)

—

” “Thu, 04 Jul 2024

**Toshiba Multi-Function Printers 40 Vulnerabilities**

103 models of Toshiba Multi-Function Printers (MFP) are vulnerable to 40 different vulnerabilities including remote code execution, local privilege escalation, xml injection, and more.

- [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
2024-07-13	AKG	[DEU]	<a href="#">Link</a>
2024-07-10	Jaboatão dos Guararapes	[BRA]	<a href="#">Link</a>
2024-07-10	Sibanye Stillwater	[ZAF]	<a href="#">Link</a>
2024-07-10	District scolaire de Goshen	[USA]	<a href="#">Link</a>
2024-07-09	Clay County Courthouse	[USA]	<a href="#">Link</a>
2024-07-09	Ville de Mahina	[FRA]	<a href="#">Link</a>
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	<a href="#">Link</a>
2024-07-04	La Ville d'Ans	[BEL]	<a href="#">Link</a>
2024-07-03	E.S.E. Salud Yopal	[COL]	<a href="#">Link</a>
2024-07-03	Florida Department of Health	[USA]	<a href="#">Link</a>
2024-07-02	Hong Kong Institute of Architects	[HKG]	<a href="#">Link</a>
2024-07-02	Apex	[USA]	<a href="#">Link</a>
2024-07-01	Hiap Seng Industries	[SGP]	<a href="#">Link</a>
2024-07-01	Monroe County government	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-13	[a-g.com - data publication 38gb (150K)]	blacksuit	<a href="#">Link</a>
2024-07-13	[gbhs.org Publication 51gb]	blacksuit	<a href="#">Link</a>
2024-07-13	[Kenya Urban Roads Authority]	hunters	<a href="#">Link</a>
2024-07-13	[Carigali Hess Operating Company]	hunters	<a href="#">Link</a>
2024-07-13	[gbhs.org 07/12 Publication 51gb]	blacksuit	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-01	[The Coffee Bean & Tea Leaf]	incransom	<a href="#">Link</a>
2024-07-01	[State of Alabama - Alabama Department Of Education]	incransom	<a href="#">Link</a>
2024-07-02	[ARISTA]	spacebears	<a href="#">Link</a>
2024-07-12	[Preferred IT Group]	bianlian	<a href="#">Link</a>
2024-07-08	[Wagner-Meinert]	ransomexx	<a href="#">Link</a>
2024-07-12	[painproclinics.com]	ransomcortex	<a href="#">Link</a>
2024-07-02	[www.zepter.de]	ransomhub	<a href="#">Link</a>
2024-07-11	[www.riteaid.com]	ransomhub	<a href="#">Link</a>
2024-07-03	[olympusgrp.com]	dispossessor	<a href="#">Link</a>
2024-07-12	[www.donaanita.com]	ransomcortex	<a href="#">Link</a>
2024-07-12	[perfeitaplastica.com.br]	ransomcortex	<a href="#">Link</a>
2024-07-12	[www.respirarlondrina.com.br]	ransomcortex	<a href="#">Link</a>
2024-07-11	[Hyperice]	play	<a href="#">Link</a>
2024-07-11	[diligentusa.com]	embargo	<a href="#">Link</a>
2024-07-11	[Image Microsystems]	blacksuit	<a href="#">Link</a>
2024-07-11	[www.lynchaluminum.com]	ransomhub	<a href="#">Link</a>
2024-07-11	[www.eurostrand.de]	ransomhub	<a href="#">Link</a>
2024-07-11	[www.netavent.dk]	ransomhub	<a href="#">Link</a>
2024-07-11	[Financoop]	akira	<a href="#">Link</a>
2024-07-11	[Sigma]	akira	<a href="#">Link</a>
2024-07-11	[Sonol ( Gas Stations )]	handala	<a href="#">Link</a>
2024-07-11	[www.bfcsolutions.com]	ransomhub	<a href="#">Link</a>
2024-07-11	[Texas Electric Cooperatives]	play	<a href="#">Link</a>
2024-07-11	[The 21st Century Energy Group]	play	<a href="#">Link</a>
2024-07-11	[T P C I]	play	<a href="#">Link</a>
2024-07-10	[City of Cedar Falls]	blacksuit	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-10	[P448]	akira	<a href="#">Link</a>
2024-07-10	[Beowulfchain]	vanirgroup	<a href="#">Link</a>
2024-07-10	[Qinao]	vanirgroup	<a href="#">Link</a>
2024-07-10	[Athlon]	vanirgroup	<a href="#">Link</a>
2024-07-10	[Usina Alta Mogiana S/A]	akira	<a href="#">Link</a>
2024-07-09	[Inland Audio Visual]	akira	<a href="#">Link</a>
2024-07-09	[Indika Energy]	hunters	<a href="#">Link</a>
2024-07-08	[Excelsior Orthopaedics]	monti	<a href="#">Link</a>
2024-07-09	[Heidmar]	akira	<a href="#">Link</a>
2024-07-03	[REPLIGEN]	incransom	<a href="#">Link</a>
2024-07-08	[Raffmetal Spa]	dragonforce	<a href="#">Link</a>
2024-07-08	[Allied Industrial Group]	akira	<a href="#">Link</a>
2024-07-08	[Esedra]	akira	<a href="#">Link</a>
2024-07-08	[Federated Co-operatives]	akira	<a href="#">Link</a>
2024-07-02	[Guhring USA]	incransom	<a href="#">Link</a>
2024-07-06	[noab.nl]	lockbit3	<a href="#">Link</a>
2024-07-07	[Strauss Brands ]	medusa	<a href="#">Link</a>
2024-07-07	[Harry Perkins Institute of medical research ]	medusa	<a href="#">Link</a>
2024-07-07	[Viasat ]	medusa	<a href="#">Link</a>
2024-07-07	[Olympus Group]	medusa	<a href="#">Link</a>
2024-07-07	[MYC Media]	rhysida	<a href="#">Link</a>
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	<a href="#">Link</a>
2024-07-03	[baiminstitute.org]	ransomhub	<a href="#">Link</a>
2024-07-05	[The Wacks Law Group]	qilin	<a href="#">Link</a>
2024-07-05	[pomalca.com.pe]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-05	[Center for Human Capital Innovation (centerforhci.org)]	incransom	<a href="#">Link</a>
2024-07-05	[waupacacounty-wi.gov]	incransom	<a href="#">Link</a>
2024-07-05	[waupaca.wi.us]	incransom	<a href="#">Link</a>
2024-07-04	[ws-stahl.eu]	lockbit3	<a href="#">Link</a>
2024-07-04	[homelandvinyl.com]	lockbit3	<a href="#">Link</a>
2024-07-04	[eicher.in]	lockbit3	<a href="#">Link</a>
2024-07-05	[National Health Laboratory Services]	blacksuit	<a href="#">Link</a>
2024-07-04	[Un Museau]	spacebears	<a href="#">Link</a>
2024-07-03	[Haylem]	spacebears	<a href="#">Link</a>
2024-07-04	[Elyria Foundry]	play	<a href="#">Link</a>
2024-07-04	[Texas Recycling]	play	<a href="#">Link</a>
2024-07-04	[INDA's]	play	<a href="#">Link</a>
2024-07-04	[Innerspec Technologies]	play	<a href="#">Link</a>
2024-07-04	[Prairie Athletic Club]	play	<a href="#">Link</a>
2024-07-04	[Fareri Associates]	play	<a href="#">Link</a>
2024-07-04	[Island Transportation Corp.]	bianlian	<a href="#">Link</a>
2024-07-04	[Legend Properties, Inc.]	bianlian	<a href="#">Link</a>
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	<a href="#">Link</a>
2024-07-03	[hcri.edu]	ransomhub	<a href="#">Link</a>
2024-07-04	[Coquitlam Concrete]	hunters	<a href="#">Link</a>
2024-07-04	[Multisuns Communication]	hunters	<a href="#">Link</a>
2024-07-04	[gerard-perrier.com]	embargo	<a href="#">Link</a>
2024-07-04	[Abileneisd.org]	cloak	<a href="#">Link</a>
2024-07-03	[sequelglobal.com]	darkvault	<a href="#">Link</a>
2024-07-03	[Explomin]	akira	<a href="#">Link</a>
2024-07-03	[Alimac]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-03	[badel1862.hr]	blackout	<a href="#">Link</a>
2024-07-03	[ramservices.com]	underground	<a href="#">Link</a>
2024-07-03	[foremedia.net]	darkvault	<a href="#">Link</a>
2024-07-03	[www.swcs-inc.com]	ransomhub	<a href="#">Link</a>
2024-07-03	[valleylandtitleco.com]	donutleaks	<a href="#">Link</a>
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>
2024-07-01	[latiusa.co.id]	lockbit3	<a href="#">Link</a>
2024-07-01	[kbc-zagreb.hr]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
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.