

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240303



## 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 . . . . .	16
<b>5 Die Hacks der Woche</b>	<b>20</b>
5.0.1 EXTRABLATT: Lockbit down? UND: ScreenConnect-Lücke (10/10 kritisch) . . .	20
<b>6 Cyberangriffe: (Mär)</b>	<b>21</b>
<b>7 Ransomware-Erpressungen: (Mär)</b>	<b>21</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

#### **Angriffe auf Windows-Lücke – Update seit einem halben Jahr verfügbar**

Die CISA warnt vor Angriffen auf eine Lücke in Microsofts Streaming Service. Updates gibt es seit mehr als einem halben Jahr.

- [Link](#)

—

#### **Sicherheitsupdate: Nvidia-Grafikkarten-Treiber als Einfallstor für Angreifer**

Angreifer können Linux- und Windows-PCs mit Nvidia-GPUs ins Visier nehmen. Es kann Schadcode auf Systeme gelangen.

- [Link](#)

—

#### **IT-Sicherheitsprodukte von Sophos verschlucken sich am Schaltjahr**

Aufgrund eines Fehlers können Sophos Endpoint, Home und Server vor dem Besuch legitimer Websites warnen. Erste Lösungen sind bereits verfügbar.

- [Link](#)

—

#### **3D-Drucker von Anycubic gehackt, um vor weiteren Hacks zu warnen**

Derzeit bekommen einige Besitzer von 3D-Druckern des Herstellers Anycubic eine Warnmeldung auf Geräte geschickt. Diese stammt aber nicht vom Hersteller.

- [Link](#)

—

#### **Cisco: Sicherheitslücken in NX-OS, FX-OS und weiteren Geräten geschlossen**

Cisco warnt vor Sicherheitslücken in mehreren Systemen und Geräten. Aktualisierungen zum Abdichten stehen bereit.

- [Link](#)

—

#### **Teamviewer: Sicherheitslücke im Client ermöglicht Rechteausweitung**

Eine Schwachstelle im Teamviewer-Client ermöglicht Nutzern, ihre Rechte im System auszuweiten. Ein Update steht bereit.

- [Link](#)

—

#### **Google Chrome: Sicherheitsupdate bessert vier Schwachstellen aus**

Googles Entwickler haben den Webbrowser Chrome in neuer Version veröffentlicht. Sie schließen damit vier Sicherheitslücken.

- [Link](#)

---

**Remote-Desktop: RustDesk-Update entfernt Test-Zertifikat**

Ein Test-Zertifikat in RustDesk für Windows führte zu Diskussionen. Ein Update entfernt es, mitsamt einiger Funktionen.

- [Link](#)

---

**Webbrowser: Microsoft Edge-Update schließt Sicherheitslücken**

Microsoft hat am Freitag den Browser Edge aktualisiert. Neben Chromium-Sicherheitslücken dichten die Entwickler auch eigene ab.

- [Link](#)

---

**Kritische Lücke in Wordpress-Plug-in Ultimate Member leakt Passwort-Hashes**

Angreifer können Wordpress-Websites mit dem Plug-in Ultimate Member attackieren. Potenziell sind mehr als 200.000 Seiten gefährdet.

- [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-2023-6895	0.901600000	0.987100000	<a href="#">Link</a>
CVE-2023-6553	0.916210000	0.988260000	<a href="#">Link</a>
CVE-2023-5360	0.967230000	0.996330000	<a href="#">Link</a>
CVE-2023-4966	0.963970000	0.995250000	<a href="#">Link</a>
CVE-2023-47246	0.943540000	0.991360000	<a href="#">Link</a>
CVE-2023-46805	0.962740000	0.994860000	<a href="#">Link</a>
CVE-2023-46747	0.972020000	0.998010000	<a href="#">Link</a>
CVE-2023-46604	0.972730000	0.998370000	<a href="#">Link</a>
CVE-2023-43177	0.932620000	0.990070000	<a href="#">Link</a>
CVE-2023-42793	0.973450000	0.998820000	<a href="#">Link</a>
CVE-2023-41265	0.915100000	0.988110000	<a href="#">Link</a>
CVE-2023-39143	0.925430000	0.989250000	<a href="#">Link</a>
CVE-2023-38646	0.904440000	0.987270000	<a href="#">Link</a>
CVE-2023-38205	0.934710000	0.990240000	<a href="#">Link</a>
CVE-2023-38203	0.949400000	0.992260000	<a href="#">Link</a>
CVE-2023-38035	0.974160000	0.999250000	<a href="#">Link</a>
CVE-2023-36845	0.966580000	0.996100000	<a href="#">Link</a>
CVE-2023-3519	0.908750000	0.987640000	<a href="#">Link</a>
CVE-2023-35082	0.934310000	0.990200000	<a href="#">Link</a>
CVE-2023-35078	0.948280000	0.992100000	<a href="#">Link</a>
CVE-2023-34960	0.925010000	0.989220000	<a href="#">Link</a>
CVE-2023-34634	0.919000000	0.988540000	<a href="#">Link</a>
CVE-2023-34362	0.959040000	0.994030000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3368	0.928930000	0.989600000	<a href="#">Link</a>
CVE-2023-33246	0.973410000	0.998770000	<a href="#">Link</a>
CVE-2023-32315	0.973960000	0.999110000	<a href="#">Link</a>
CVE-2023-30625	0.951530000	0.992590000	<a href="#">Link</a>
CVE-2023-30013	0.937480000	0.990580000	<a href="#">Link</a>
CVE-2023-29300	0.963530000	0.995110000	<a href="#">Link</a>
CVE-2023-29298	0.921360000	0.988760000	<a href="#">Link</a>
CVE-2023-28771	0.923800000	0.989080000	<a href="#">Link</a>
CVE-2023-28121	0.925190000	0.989250000	<a href="#">Link</a>
CVE-2023-27524	0.972470000	0.998280000	<a href="#">Link</a>
CVE-2023-27372	0.971580000	0.997810000	<a href="#">Link</a>
CVE-2023-27350	0.972270000	0.998200000	<a href="#">Link</a>
CVE-2023-26469	0.938970000	0.990770000	<a href="#">Link</a>
CVE-2023-26360	0.960730000	0.994440000	<a href="#">Link</a>
CVE-2023-26035	0.969370000	0.996990000	<a href="#">Link</a>
CVE-2023-25717	0.962180000	0.994710000	<a href="#">Link</a>
CVE-2023-2479	0.963310000	0.995040000	<a href="#">Link</a>
CVE-2023-24489	0.973430000	0.998800000	<a href="#">Link</a>
CVE-2023-23752	0.948570000	0.992150000	<a href="#">Link</a>
CVE-2023-23397	0.917330000	0.988370000	<a href="#">Link</a>
CVE-2023-22527	0.965680000	0.995850000	<a href="#">Link</a>
CVE-2023-22518	0.969180000	0.996930000	<a href="#">Link</a>
CVE-2023-22515	0.973330000	0.998730000	<a href="#">Link</a>
CVE-2023-21839	0.960490000	0.994400000	<a href="#">Link</a>
CVE-2023-21554	0.961220000	0.994510000	<a href="#">Link</a>
CVE-2023-20887	0.965640000	0.995830000	<a href="#">Link</a>
CVE-2023-20198	0.919220000	0.988560000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-1671	0.964250000	0.995340000	<a href="#">Link</a>
CVE-2023-0669	0.968020000	0.996580000	<a href="#">Link</a>

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

Fri, 01 Mar 2024

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

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

- [Link](#)

—

Fri, 01 Mar 2024

#### **[NEU] [hoch] SolarWinds Security Event Manager: Mehrere Schwachstellen**

Ein entfernter, anonymer oder authentifizierter Angreifer kann mehrere Schwachstellen in SolarWinds Security Event Manager ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 01 Mar 2024

#### **[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 01 Mar 2024

#### **[NEU] [hoch] Dell Data Protection Advisor: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Dell Data Protection Advisor ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen, seine Berechtigungen zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)



—  
Fri, 01 Mar 2024

**[UPDATE] [hoch] Node.js: Mehrere Schwachstellen**

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

- [Link](#)

—  
Fri, 01 Mar 2024

**[NEU] [hoch] Triumph-Adler aQrate: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Triumph-Adler aQrate ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—  
Fri, 01 Mar 2024

**[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, Sicherheitsmaßnahmen zu umgehen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—  
Fri, 01 Mar 2024

**[NEU] [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](#)

—  
Fri, 01 Mar 2024

**[NEU] [hoch] IBM MQ: Mehrere Schwachstellen**

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

- [Link](#)

—

Fri, 01 Mar 2024

**[NEU] [hoch] Dell integrated Dell Remote Access Controller: Schwachstelle ermöglicht Privilegieneskalation**

Ein authentisierter Angreifer aus dem angrenzenden Netzbereich kann eine Schwachstelle in Dell integrated Dell Remote Access Controller ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 01 Mar 2024

**[UPDATE] [hoch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Rechte zu erweitern, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, Daten zu Manipulieren und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 01 Mar 2024

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

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

- [Link](#)

—

Fri, 01 Mar 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux (Pillow): Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux in der Komponente "Pillow" ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 01 Mar 2024

**[UPDATE] [hoch] Autodesk AutoCAD: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Autodesk AutoCAD ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 01 Mar 2024

**[UPDATE] [hoch] Adobe Acrobat: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe Acrobat, Adobe Acrobat Reader, Adobe Acrobat DC und Adobe Acrobat Reader DC ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder Informationen offenzulegen.

- [Link](#)

—

Thu, 29 Feb 2024

**[NEU] [hoch] Progress Software Sitefinity: Mehrere Schwachstellen**

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Progress Software Sitefinity ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen offenzulegen oder Cross-Site Scripting (XSS)-Angriffe durchzuführen.

- [Link](#)

—

Thu, 29 Feb 2024

**[NEU] [hoch] Cisco NX-OS: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Cisco NX-OS ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Thu, 29 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform ausnutzen, um beliebigen Programmcode auszuführen, ein Cross-Site-Scripting-Angriff durchzuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 29 Feb 2024

**[UPDATE] [hoch] Red Hat Integration Camel for Spring Boot: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Integration Camel for Spring Boot ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gefährden.

- [Link](#)

—

Thu, 29 Feb 2024

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

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/1/2024	[Debian dla-3745 : gsoap - security update]	critical
2/29/2024	[Siemens SINEC NMS < V2.0 SP1 Multiple Vulnerabilities]	critical
2/29/2024	[Tenable Identity Exposure < 3.59.4 Multiple Vulnerabilities (TNS-2024-04)]	critical
3/2/2024	[Fedora 39 : dotnet8.0 (2024-a2b7ec0ba4)]	high
3/2/2024	[Fedora 39 : mod_auth_openidc (2024-3c0f2a2771)]	high
3/2/2024	[Fedora 38 : dotnet8.0 (2024-b2db508cc2)]	high
3/2/2024	[openSUSE 15 Security Update : openvswitch3 (SUSE-SU-2024:0738-1)]	high
3/2/2024	[Fedora 39 : dhcpcd (2024-e1fc365e53)]	high
3/1/2024	[SUSE SLES15 Security Update : nodejs14 (SUSE-SU-2024:0732-1)]	high
3/1/2024	[SUSE SLES15 Security Update : kernel (Live Patch 18 for SLE 15 SP4) (SUSE-SU-2024:0685-1)]	high
3/1/2024	[SUSE SLES15 Security Update : kernel (Live Patch 41 for SLE 15 SP3) (SUSE-SU-2024:0695-1)]	high
3/1/2024	[SUSE SLES15 / openSUSE 15 Security Update : nodejs18 (SUSE-SU-2024:0730-1)]	high
3/1/2024	[SUSE SLES12 / SLES15 Security Update : kernel (Live Patch 10 for SLE 15 SP4) (SUSE-SU-2024:0698-1)]	high
3/1/2024	[SUSE SLES15 Security Update : kernel (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2024:0727-1)]	high
3/1/2024	[SUSE SLES15 Security Update : nodejs12 (SUSE-SU-2024:0733-1)]	high
3/1/2024	[SUSE SLES12 Security Update : nodejs16 (SUSE-SU-2024:0731-1)]	high
3/1/2024	[SUSE SLES15 Security Update : kernel (Live Patch 20 for SLE 15 SP4) (SUSE-SU-2024:0694-1)]	high

Datum	Schwachstelle	Bewertung
3/1/2024	[SUSE SLES15 Security Update : kernel (Live Patch 37 for SLE 15 SP3) (SUSE-SU-2024:0705-1)]	high
3/1/2024	[Debian dla-3746 : libwireshark-data - security update]	high
3/1/2024	[Fedora 38 : dotnet7.0 (2024-04b568cd49)]	high
3/1/2024	[Fedora 38 : gifsicle (2024-4672c1ff2d)]	high
3/1/2024	[Nagios XI < 2024R1.0.2 Multiple Vulnerabilities]	high
3/1/2024	[Oracle Linux 8 : kernel (ELSA-2024-12187)]	high
3/1/2024	[Cisco Nexus 3600 External BGP DoS (cisco-sa-nxos-po-acl-TkyePgVL)]	high
3/1/2024	[Atlassian Confluence 6.0.1 < 7.19.18 / 7.20.x < 8.5.5 / 8.6.x < 8.7.2 / 8.8.0 (CONFSERVER-94111)]	high
3/1/2024	[Cisco NX-OS Software MPLS Encapsulated IPv6 DoS (cisco-sa-ipv6-mpls-dos-R9ycXkwM)]	high
3/1/2024	[FreeBSD : NodeJS – Vulnerabilities (77a6f1c9-d7d2-11ee-bb12-001b217b3468)]	high
2/29/2024	[RHEL 7 : go-toolset-1.19-golang (RHSA-2024:1041)]	high
2/29/2024	[Debian dla-3744 : python-django - security update]	high
2/29/2024	[RHEL 8 : python-pillow (RHSA-2024:1060)]	high
2/29/2024	[RHEL 8 : python-pillow (RHSA-2024:1059)]	high
2/29/2024	[RHEL 8 : python-pillow (RHSA-2024:1058)]	high
2/29/2024	[RHEL 9 : kpatch-patch (RHSA-2024:1055)]	high
2/29/2024	[Microsoft Edge (Chromium) < 122.0.2365.63 Multiple Vulnerabilities]	high
2/29/2024	[FreeBSD : electron{27,28} – Use after free in Mojo (3567456a-6b17-41f7-ba7f-5cd3efb2b7c9)]	high
2/29/2024	[FreeBSD : chromium – multiple security fixes (31bb1b8d-d6dc-11ee-86bb-a8a1599412c6)]	high
2/29/2024	[Fedora 39 : dotnet7.0 (2024-a66f05d20f)]	high
2/29/2024	[Fedora 39 : gifsicle (2024-5e50570506)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Fri, 01 Mar 2024

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

This archive contains all of the 106 exploits added to Packet Storm in February, 2024.

- [Link](#)

—

” “Fri, 01 Mar 2024

#### ***BoidCMS 2.0.0 Command Injection***

This Metasploit module leverages CVE-2023-38836, an improper sanitization bug in BoidCMS versions 2.0.0 and below. BoidCMS allows the authenticated upload of a php file as media if the file has the GIF header, even if the file is a php file.

- [Link](#)

—

” “Fri, 01 Mar 2024

#### ***Membership Management System 1.0 SQL Injection***

Membership Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Thu, 29 Feb 2024

#### ***Backdoor.Win32.Agent.amt MVID-2024-0673 Authentication Bypass / Code Execution***

Backdoor.Win32.Agent.amt malware suffers from bypass and code execution vulnerabilities.

- [Link](#)

—

” “Thu, 29 Feb 2024

#### ***Backdoor.Win32.Jeemp.c MVID-2024-0672 Hardcoded Credential***

Backdoor.Win32.Jeemp.c malware suffers from a hardcoded credential vulnerability.

- [Link](#)

—

” “Thu, 29 Feb 2024

#### ***WordPress IDonate Blood Request Management System 1.8.1 Cross Site Scripting***

WordPress IDonate Blood Request Management System plugin versions 1.8.1 and below suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Wed, 28 Feb 2024

**Telegram For Android Connection::onReceivedData Use-After-Free**

In the tgnet library used in Telegram messenger for Android, there is a use-after-free vulnerability in Connection::onReceivedData that can be triggered remotely.

- [Link](#)

—

” “Wed, 28 Feb 2024

**Saflok System 6000 Key Derivation**

This is a key derivation exploit for Saflokk System 6000.

- [Link](#)

—

” “Wed, 28 Feb 2024

**Blood Bank 1.0 SQL Injection**

Blood Bank version 1.0 suffers from multiple remote SQL injection vulnerabilities. Original discovery of SQL injection in this version is attributed to Nitin Sharma in October of 2021.

- [Link](#)

—

” “Wed, 28 Feb 2024

**WordPress WP Fastest Cache 1.2.2 SQL Injection**

WordPress WP Fastest Cache plugin version 1.2.2 suffers from an unauthenticated remote SQL injection vulnerability.

- [Link](#)

—

” “Wed, 28 Feb 2024

**WordPress Admin Bar And Dashboard Access Control 1.28 XSS**

WordPress Admin Bar and Dashboard Access Control plugin version 1.28 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

**Hospital Management System 1.0 Insecure Direct Object Reference / Account Takeover**

Hospital Management System version 1.0 suffers from insecure direct object reference and account takeover vulnerabilities.

- [Link](#)

—

” “Tue, 27 Feb 2024

**Hospital Management System 1.0 Cross Site Scripting**

Hospital Management System version 1.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

***Hospital Management System 1.0 SQL Injection***

Hospital Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

***perl2exe 30.10C Arbitrary Code Execution***

Executables created with perl2exe versions 30.10C and below suffer from an arbitrary code execution vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

***Automatic-Systems SOC FL9600 FastLine Hardcoded Credentials***

Automatic-Systems SOC FL9600 FastLine version V06 has hardcoded credentials for super admin functionality.

- [Link](#)

—

” “Tue, 27 Feb 2024

***Automatic-Systems SOC FL9600 FastLine Directory Traversal***

Automatic-Systems SOC FL9600 FastLine version V06 suffers from a directory traversal vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

***Atlassian Confluence Data Center And Server Authentication Bypass***

This Metasploit module exploits a broken access control vulnerability in Atlassian Confluence servers leading to an authentication bypass. A specially crafted request can be create new admin account without authentication on the target Atlassian server.

- [Link](#)

—

” “Tue, 27 Feb 2024

***Moodle 4.3 Insecure Direct Object Reference***

Moodle version 4.3 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “Tue, 27 Feb 2024

***WordPress Canto Remote Shell Upload***

WordPress Canto versions prior to 3.0.5 suffer from remote file inclusion and shell upload vulnerabili-



ties.

- [Link](#)

—

” “Tue, 27 Feb 2024

***WordPress Comments Like Dislike 1.2.0 Missing Authorization***

WordPress Comments Like Dislike plugin versions 1.2.0 and below suffer from a missing capability check on the `restore_settings` function that allows an attacker to reset the plugin’s settings.

- [Link](#)

—

” “Tue, 27 Feb 2024

***SuperStoreFinder 3.7 XSS / CSRF / Command Execution***

SuperStoreFinder versions 3.7 and below suffer from cross site request forgery, remote command execution, and remote SQL injection vulnerabilities.

- [Link](#)

—

” “Mon, 26 Feb 2024

***Simple Inventory Management System 1.0 SQL Injection***

Simple Inventory Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 26 Feb 2024

***Flashcard Quiz App 1.0 SQL Injection***

Flashcard Quiz App version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 26 Feb 2024

***FAQ Management System 1.0 SQL Injection***

FAQ Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

”

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

“Fri, 01 Mar 2024

***ZDI-24-229: Linux Kernel ksmdb Session Key Exchange Heap-based Buffer Overflow Remote Code Execution Vulnerability***

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-228: Linux Kernel ksmbd Negotiate Request Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-227: Linux Kernel ksmbd Chained Request Improper Input Validation Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-226: Kofax Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-225: Kofax Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-224: Kofax Power PDF PDF File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-223: Kofax Power PDF PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-222: Kofax Power PDF PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-221: Kofax Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Executi-**

**on Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-220: Kofax Power PDF PDF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-219: Kofax Power PDF app response Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-218: Kofax Power PDF PNG File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-217: Kofax Power PDF PNG File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-216: Kofax Power PDF GIF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Fri, 01 Mar 2024

**ZDI-24-215: SolarWinds Security Event Manager AMF Deserialization of Untrusted Data Remote Code Execution Vulnerability**

- [Link](#)

—

” “Wed, 28 Feb 2024

**ZDI-24-214: NI FlexLogger RabbitMQ Incorrect Permission Assignment Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 28 Feb 2024

**ZDI-24-213: NI FlexLogger userservices Missing Authorization Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 28 Feb 2024

**ZDI-24-212: NI FlexLogger TagHistorian Missing Authorization Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 28 Feb 2024

**ZDI-24-211: NI FlexLogger DocumentManager Missing Authorization Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 28 Feb 2024

**ZDI-24-210: NI FlexLogger SkylineService Missing Authorization Local Privilege Escalation Vulnerability**

- [Link](#)

—

” “Wed, 28 Feb 2024

**ZDI-24-209: NI FlexLogger ServiceRegistry Missing Authorization Local Privilege Escalation Vulnerability**

- [Link](#)

—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 EXTRABLATT: Lockbit down? UND: ScreenConnect-Lücke (10/10 kritisch)



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Mär)

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

## 7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-03	[stockdevelopment.com]	lockbit3	<a href="#">Link</a>
2024-03-03	[Ewig Usa]	alphv	<a href="#">Link</a>
2024-03-02	[aerospace.com]	lockbit3	<a href="#">Link</a>
2024-03-02	[starkpower.de]	lockbit3	<a href="#">Link</a>
2024-03-02	[roehr-stolberg.de]	lockbit3	<a href="#">Link</a>
2024-03-02	[schuett-grundei.de]	lockbit3	<a href="#">Link</a>
2024-03-02	[unitednotions.com]	lockbit3	<a href="#">Link</a>
2024-03-02	[smuldes.com]	lockbit3	<a href="#">Link</a>
2024-03-02	[esser-ps.de]	lockbit3	<a href="#">Link</a>
2024-03-01	[SBM & Co [You have 48 hours. Check your e-mail]]	alphv	<a href="#">Link</a>
2024-03-01	[Skyland Grain]	play	<a href="#">Link</a>
2024-03-01	[American Nuts]	play	<a href="#">Link</a>
2024-03-01	[A&A Wireless]	play	<a href="#">Link</a>
2024-03-01	[Powill Manufacturing & Engineering]	play	<a href="#">Link</a>
2024-03-01	[Trans+Plus Systems]	play	<a href="#">Link</a>
2024-03-01	[Hedlunds]	play	<a href="#">Link</a>
2024-03-01	[Red River Title]	play	<a href="#">Link</a>
2024-03-01	[Compact Mould]	play	<a href="#">Link</a>
2024-03-01	[Winona Pattern & Mold]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-01	[Marketon]	play	<a href="#">Link</a>
2024-03-01	[Stack Infrastructure]	play	<a href="#">Link</a>
2024-03-01	[Coastal Car]	play	<a href="#">Link</a>
2024-03-01	[New Bedford Welding Supply]	play	<a href="#">Link</a>
2024-03-01	[Influence Communication]	play	<a href="#">Link</a>
2024-03-01	[Kool-air]	play	<a href="#">Link</a>
2024-03-01	[FBI Construction]	play	<a href="#">Link</a>
2024-03-01	[SBM & Co]	alphv	<a href="#">Link</a>
2024-03-01	[Shooting House ]	ransomhub	<a href="#">Link</a>
2024-03-01	[Crystal Window & Door Systems]	dragonforce	<a href="#">Link</a>
2024-03-01	[Gilmore Construction]	blacksuit	<a href="#">Link</a>
2024-03-01	[Petrus Resources Ltd]	alphv	<a href="#">Link</a>
2024-03-01	[CoreData]	akira	<a href="#">Link</a>
2024-03-01	[Gansevoort Hotel Group]	akira	<a href="#">Link</a>
2024-03-01	[DJI Company]	mogilevich	<a href="#">Link</a>
2024-03-01	[Kick]	mogilevich	<a href="#">Link</a>
2024-03-01	[Shein]	mogilevich	<a href="#">Link</a>
2024-03-01	[Kumagai Gumi Group]	alphv	<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.