

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240816



## 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 . . . . .	17
<b>5 Die Hacks der Woche</b>	<b>21</b>
5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . .	21
<b>6 Cyberangriffe: (Aug)</b>	<b>22</b>
<b>7 Ransomware-Erpressungen: (Aug)</b>	<b>22</b>
<b>8 Quellen</b>	<b>29</b>
8.1 Quellenverzeichnis . . . . .	29
<b>9 Impressum</b>	<b>31</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

#### ***Solarwinds Web Help Desk: Schadcode kann Host-System infizieren***

Eine nun geschlossene kritische Sicherheitslücke bedrohte die Kundensupport-Software Web Help Desk von Solarwinds.

- [Link](#)

—

#### ***IBM-Entwickler schließen Schadcode-Lücken in AIX und App Connect***

Unternehmen mit IBM-Software sollten ihre Systeme aus Sicherheitsgründen auf den aktuellen Stand bringen.

- [Link](#)

—

#### ***Ivanti schließt unter anderem Admin-Lücke in Virtual Traffic Manager***

Kritische Sicherheitslücken bedrohen Produkte von Ivanti. Noch sind keine Attacken bekannt. Noch sind nicht alle Updates verfügbar.

- [Link](#)

—

#### ***Patchday Adobe: Acrobat, Illustrator & Co. als Schlupfloch für Schadcode***

Adobe stuft mehrere Sicherheitslücken in seinen Produkten als kritisch ein. Sicherheitsupdates sind verfügbar.

- [Link](#)

—

#### ***Patchday Microsoft: Angreifer attackieren Office und Windows mit Schadcode***

Es sind wichtige Sicherheitsupdates für verschiedene Microsoft-Produkte erschienen. Aufgrund von laufenden Attacken sollten Admins zügig handeln.

- [Link](#)

—

#### ***Patchday: Angreifer können SAP BusinessObjects kompromittieren***

Die SAP-Entwickler haben unter anderem kritische Sicherheitslücken in ihrer Unternehmenssoftware geschlossen.

- [Link](#)

—

#### ***Sicherheitslücken: Netzwerkmonitoringtool Zabbix kann Passwörter leaken***

Unter anderen eine kritische Schadcode-Lücke bedroht Zabbix. Dagegen abgesicherte Versionen stehen zum Download bereit.

- [Link](#)

---

**Root-Sicherheitslücke bedroht Datenbankmanagementsystem PostgreSQL**

Die PostgreSQL-Entwickler haben in aktuellen Versionen eine Schwachstelle geschlossen. Angreifer können Schadcode ausführen.

- [Link](#)

---

**VPN-Clients und Passwortmanager betroffen: Klartextpasswort im Prozessspeicher**

Wegen einer Lücke unter anderem in VPN-Clients und Passwortmanagern bleiben vertrauliche Daten auch nach Abmeldung im Prozess-Speicher und sind auslesbar.

- [Link](#)

---

**CPU-Sicherheitslücke in AMD-Prozessoren ermöglicht Malware-Infektionen**

Sicherheitsforscher haben eine als Sinkclose bezeichnete Sicherheitslücke in AMD-CPU's entdeckt und auf der Defcon 32 in Las Vegas präsentiert.

- [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	0.921160000	0.989990000	<a href="#">Link</a>
CVE-2023-6553	0.927320000	0.990700000	<a href="#">Link</a>
CVE-2023-5360	0.902780000	0.988720000	<a href="#">Link</a>
CVE-2023-52251	0.944080000	0.992540000	<a href="#">Link</a>
CVE-2023-4966	0.971280000	0.998290000	<a href="#">Link</a>
CVE-2023-49103	0.962110000	0.995600000	<a href="#">Link</a>
CVE-2023-48795	0.964660000	0.996190000	<a href="#">Link</a>
CVE-2023-47246	0.959010000	0.995000000	<a href="#">Link</a>
CVE-2023-46805	0.937250000	0.991710000	<a href="#">Link</a>
CVE-2023-46747	0.972820000	0.998890000	<a href="#">Link</a>
CVE-2023-46604	0.961790000	0.995530000	<a href="#">Link</a>
CVE-2023-4542	0.928310000	0.990790000	<a href="#">Link</a>
CVE-2023-43208	0.972240000	0.998630000	<a href="#">Link</a>
CVE-2023-43177	0.964550000	0.996170000	<a href="#">Link</a>
CVE-2023-42793	0.969020000	0.997460000	<a href="#">Link</a>
CVE-2023-41265	0.911110000	0.989280000	<a href="#">Link</a>
CVE-2023-39143	0.939130000	0.991960000	<a href="#">Link</a>
CVE-2023-38646	0.906610000	0.988960000	<a href="#">Link</a>
CVE-2023-38205	0.953670000	0.994110000	<a href="#">Link</a>
CVE-2023-38203	0.966410000	0.996710000	<a href="#">Link</a>
CVE-2023-38146	0.920720000	0.989940000	<a href="#">Link</a>
CVE-2023-38035	0.974680000	0.999700000	<a href="#">Link</a>
CVE-2023-36845	0.966270000	0.996670000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965340000	0.996430000	<a href="#">Link</a>
CVE-2023-35082	0.966130000	0.996630000	<a href="#">Link</a>
CVE-2023-35078	0.970440000	0.997950000	<a href="#">Link</a>
CVE-2023-34993	0.972640000	0.998800000	<a href="#">Link</a>
CVE-2023-34960	0.928290000	0.990790000	<a href="#">Link</a>
CVE-2023-34634	0.925130000	0.990480000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988960000	<a href="#">Link</a>
CVE-2023-34362	0.971000000	0.998170000	<a href="#">Link</a>
CVE-2023-34039	0.947770000	0.993070000	<a href="#">Link</a>
CVE-2023-3368	0.932420000	0.991260000	<a href="#">Link</a>
CVE-2023-33246	0.972040000	0.998520000	<a href="#">Link</a>
CVE-2023-32315	0.970550000	0.998000000	<a href="#">Link</a>
CVE-2023-30625	0.953800000	0.994130000	<a href="#">Link</a>
CVE-2023-30013	0.962380000	0.995650000	<a href="#">Link</a>
CVE-2023-29300	0.968930000	0.997440000	<a href="#">Link</a>
CVE-2023-29298	0.947600000	0.993050000	<a href="#">Link</a>
CVE-2023-28432	0.906190000	0.988920000	<a href="#">Link</a>
CVE-2023-28343	0.942300000	0.992320000	<a href="#">Link</a>
CVE-2023-28121	0.909500000	0.989140000	<a href="#">Link</a>
CVE-2023-27524	0.970600000	0.998020000	<a href="#">Link</a>
CVE-2023-27372	0.972120000	0.998570000	<a href="#">Link</a>
CVE-2023-27350	0.969720000	0.997730000	<a href="#">Link</a>
CVE-2023-26469	0.956020000	0.994560000	<a href="#">Link</a>
CVE-2023-26360	0.965230000	0.996390000	<a href="#">Link</a>
CVE-2023-26035	0.967360000	0.996980000	<a href="#">Link</a>
CVE-2023-25717	0.954250000	0.994220000	<a href="#">Link</a>
CVE-2023-25194	0.968820000	0.997410000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963740000	0.995960000	<a href="#">Link</a>
CVE-2023-24489	0.973870000	0.999310000	<a href="#">Link</a>
CVE-2023-23752	0.956380000	0.994600000	<a href="#">Link</a>
CVE-2023-23333	0.958950000	0.994990000	<a href="#">Link</a>
CVE-2023-22527	0.968290000	0.997240000	<a href="#">Link</a>
CVE-2023-22518	0.965970000	0.996570000	<a href="#">Link</a>
CVE-2023-22515	0.973250000	0.999050000	<a href="#">Link</a>
CVE-2023-21839	0.955020000	0.994360000	<a href="#">Link</a>
CVE-2023-21554	0.952830000	0.993960000	<a href="#">Link</a>
CVE-2023-20887	0.970670000	0.998040000	<a href="#">Link</a>
CVE-2023-1671	0.962480000	0.995660000	<a href="#">Link</a>
CVE-2023-0669	0.969440000	0.997610000	<a href="#">Link</a>

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

Thu, 15 Aug 2024

**[NEU] [hoch] Red Hat Enterprise Linux (Fence Agents Remediation): Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 15 Aug 2024

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

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

- [Link](#)

—



Thu, 15 Aug 2024

**[UPDATE] [UNGEPATCHT] [hoch] Ivanti Connect Secure und Fortinet FortiGate: Mehrere Schwachstellen ermöglichen Manipulation von Dateien und die Offenlegung von Informationen**

Ein Angreifer mit Zugriff auf das System kann mehrere Schwachstellen in Ivanti Connect Secure und Fortinet FortiGate ausnutzen, um Dateien zu manipulieren und vertrauliche Informationen preiszugeben.

- [Link](#)

—

Thu, 15 Aug 2024

**[NEU] [hoch] PaloAlto Networks Cortex XSOAR: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PaloAlto Networks Cortex XSOAR ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 15 Aug 2024

**[UPDATE] [hoch] Intel Ethernet Controller: Mehrere Schwachstellen ermöglichen Privilegieneskalation und Denial of Service**

Ein lokaler oder entfernter anonymer Angreifer kann mehrere Schwachstellen in Intel Ethernet Controller ausnutzen, um seine Privilegien zu erhöhen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Thu, 15 Aug 2024

**[UPDATE] [hoch] Intel Server Board S2600ST Family Firmware: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle in der Intel Server Board S2600ST Family Firmware ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Thu, 15 Aug 2024

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 15 Aug 2024

**[UPDATE] [hoch] Jenkins Plugins: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Jenkins Plugins ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren, einen Cross-Site-Scripting-Angriff durchzuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 15 Aug 2024

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

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

- [Link](#)

—

Thu, 15 Aug 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](#)

—

Thu, 15 Aug 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](#)

—

Thu, 15 Aug 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- [Link](#)

—

Thu, 15 Aug 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](#)

—

Thu, 15 Aug 2024

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

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

- [Link](#)

—

Thu, 15 Aug 2024

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

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

- [Link](#)

—

Thu, 15 Aug 2024

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

Ein entfernter, anonym oder lokaler 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](#)

—

Thu, 15 Aug 2024

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

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

- [Link](#)

—

Thu, 15 Aug 2024

**[UPDATE] [hoch] Red Hat Enterprise Linux (python-setuptools): Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonym oder lokaler Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 15 Aug 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Jenkins ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 14 Aug 2024

**[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen**

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

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/15/2024	[Kibana 7.7.x < 7.17.23 / 8.0.x < 8.14.2 (ESA-2024-22)]	critical
8/15/2024	[Adobe Reader < 20.005.30655 / 24.002.21005 Multiple Vulnerabilities (APSB24-57) (macOS)]	critical
8/15/2024	[Adobe Acrobat < 20.005.30655 / 24.001.30159 / 24.002.21005 Multiple Vulnerabilities (APSB24-57)]	critical
8/15/2024	[Adobe Acrobat < 20.005.30655 / 24.001.30159 / 24.002.21005 Multiple Vulnerabilities (APSB24-57) (macOS)]	critical
8/15/2024	[Adobe Reader < 20.005.30655 / 24.002.21005 Multiple Vulnerabilities (APSB24-57)]	critical
8/15/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-5402)]	critical
8/15/2024	[Security Update for Microsoft Project RCE (August 2024)]	critical
8/15/2024	[SolarWinds Web Help Desk < 12.8.3 HF 1 Deserialization RCE]	critical
8/15/2024	[F5 Networks BIG-IP : Apache HTTPD vulnerabilities (K000140620)]	critical
8/15/2024	[RHEL 9 : firefox (RHSA-2024:5322)]	critical
8/15/2024	[RHEL 9 : Red Hat JBoss Enterprise Application Platform 8.0.3 Security update (Important) (RHSA-2024:5481)]	critical
8/15/2024	[RHEL 8 : Red Hat JBoss Enterprise Application Platform 8.0.3 Security update (Important) (RHSA-2024:5479)]	critical

Datum	Schwachstelle	Bewertung
8/15/2024	[Fedora 39 : thunderbird (2024-7fe5206574)]	critical
8/15/2024	[Security Updates for Microsoft PowerPoint Products (August 2024)]	high
8/15/2024	[Adobe Substance 3D Designer < 14.0 (apsb24-67)]	high
8/15/2024	[ManageEngine ADAudit Plus < Build 8003 Multiple Vulnerabilities]	high
8/15/2024	[ManageEngine ADAudit Plus < Build 8110 Multiple Vulnerabilities]	high
8/15/2024	[Oracle Linux 9 : kernel (ELSA-2024-5363)]	high
8/15/2024	[Dell Peripheral Manager < 1.7.6 Multiple Vulnerabilities (DSA-2024-242)]	high
8/15/2024	[MongoDB 5.0.x < 5.0.27 / 6.0.x < 6.0.16 / 7.0.x < 7.0.12 / 7.3.x < 7.3.3 (SERVER-93211)]	high
8/15/2024	[F5 Networks BIG-IP : BIG-IP TMM vulnerability (K000138833)]	high
8/15/2024	[F5 Networks BIG-IP : BIG-IP HSB vulnerability (K05710614)]	high
8/15/2024	[F5 Networks BIG-IP : Apache HTTP server vulnerability (K000140693)]	high
8/15/2024	[Fedora 39 : roundcubemail (2024-b60eb661a4)]	high
8/15/2024	[Fedora 39 : 389-ds-base (2024-c8290315df)]	high
8/15/2024	[Fedora 39 : dotnet8.0 (2024-70741fe21f)]	high
8/15/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : GNOME Shell vulnerability (USN-6963-1)]	high
8/15/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : LibreOffice vulnerability (USN-6962-1)]	high
8/15/2024	[RHEL 9 : bind and bind-dyndb-ldap (RHSA-2024:5231)]	high
8/15/2024	[RHEL 9 : kernel (RHSA-2024:5363)]	high
8/15/2024	[RHEL 9 : python3.11-setuptools (RHSA-2024:5279)]	high
8/15/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : ORC vulnerability (USN-6964-1)]	high

Datum	Schwachstelle	Bewertung
8/15/2024	[Fedora 39 : tor (2024-c2da7f4de7)]	high
8/15/2024	[Ubuntu 16.04 LTS : Bind vulnerabilities (USN-6909-3)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Thu, 15 Aug 2024

#### **LG Simple Editor 3.21.0 Command Injection**

LG Simple Editor versions 3.21.0 and below suffer from an unauthenticated command injection vulnerability. The vulnerability can be exploited by a remote attacker to inject arbitrary operating system commands which will get executed in the context of NT AUTHORITY\SYSTEM.

- [Link](#)

—

” “Thu, 15 Aug 2024

#### **OpenMetadata 1.2.3 Authentication Bypass / SpEL Injection**

This Metasploit module exploits OpenMetadata versions 1.2.3 and below by chaining an API authentication bypass using JWT tokens along with a SpEL injection vulnerability to achieve arbitrary command execution.

- [Link](#)

—

” “Thu, 15 Aug 2024

#### **Apache HugeGraph Gremlin Remote Code Execution**

This Metasploit module exploits CVE-2024-27348, a remote code execution vulnerability that exists in Apache HugeGraph Server in versions before 1.3.0. An attacker can bypass the sandbox restrictions and achieve remote code execution through Gremlin, resulting in complete control over the server.

- [Link](#)

—

” “Thu, 15 Aug 2024

#### **Feberr 13.4 Insecure Settings**

Feberr version 13.4 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***Farmacia Gama 1.0 Cross Site Scripting***

Farmacia Gama version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***Ecommerce 1.15 Insecure Settings***

Ecommerce version 1.15 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***Covid-19 Contact Tracing System 1.0 Cross Site Scripting***

Covid-19 Contact Tracing System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***Car Rental Management System 1.0 Cross Site Scripting***

Car Rental Management System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***BloodBank 1.1 Insecure Settings***

BloodBank version 1.1 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***Bhojon Restaurant Management System 2.9 Insecure Settings***

Bhojon Restaurant Management System version 2.9 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Thu, 15 Aug 2024

***FlatPress 1.3.1 Path Traversal***

FlatPress version 1.3.1 suffers from a path traversal vulnerability.

- [Link](#)

—

” “Wed, 14 Aug 2024

***K7 Ultimate Security NULL Pointer Dereference***

In K7 Ultimate Security versions prior to 17.0.2019, the driver file (K7RKScan.sys - this version 15.1.0.7)

allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of a null pointer dereference from IOCTL 0x222010 and 0x222014. At the same time, the drive is accessible to all users in the "Everyone" group.

- [Link](#)

—

" "Wed, 14 Aug 2024

#### **Microsoft CLFS.sys Denial of Service**

CVE-2024-6768 is a vulnerability in the Common Log File System (CLFS.sys) driver of Windows, caused by improper validation of specified quantities in input data. This flaw leads to an unrecoverable inconsistency, triggering the KeBugCheckEx function and resulting in a Blue Screen of Death (BSOD). The issue affects all versions of Windows 10 and Windows 11, Windows Server 2016, Server 2019 and Server 2022 despite having all updates applied. This Proof of Concept (PoC) shows that by crafting specific values within a .BLF file, an unprivileged user can induce a system crash.

- [Link](#)

—

" "Wed, 14 Aug 2024

#### **Kortex 1.0 Insecure Direct Object Reference**

Kortex version 1.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

" "Wed, 14 Aug 2024

#### **Job Castle 1.0 Arbitrary File Upload**

Job Castle version 1.0 suffers from an arbitrary file upload vulnerability.

- [Link](#)

—

" "Wed, 14 Aug 2024

#### **Hotel Management System 1.0 Arbitrary File Upload**

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

- [Link](#)

—

" "Wed, 14 Aug 2024

#### **Covid-19 Contact Tracing System 1.0 SQL Injection**

Covid-19 Contact Tracing System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

" "Wed, 14 Aug 2024

#### **Car Listing 1.6 Insecure Settings**



Car Listing version 1.6 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Wed, 14 Aug 2024

**MalwareBytes 19 Arbitrary File Deletion / Privilege Escalation**

Malwarebytes is prone to an arbitrary file deletion (usage of DeleteFileW by MBAMService.exe) running as SYSTEM. This process can be manipulated from a non-admin user because it fails to properly filter the user supplied input while scanning a file, this vulnerability leads to a privilege escalation. This exploit was tested on Windows 10 Pro version 22H2 (OS Build 19045.4412). Versions 19 and below are affected.

- [Link](#)

—

” “Tue, 13 Aug 2024

**WordPress MapFig Studio 0.2.1 Cross Site Request Forgery / Cross Site Scripting**

WordPress MapFig Studio plugin versions 0.2.1 and below suffer from cross site request forgery and cross site scripting vulnerabilities.

- [Link](#)

—

” “Tue, 13 Aug 2024

**WordPress Profilepro 1.3 Cross Site Scripting**

WordPress Profilepro plugin versions 1.3 and below suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 13 Aug 2024

**WordPress Light Poll 1.0.0 Cross Site Request Forgery**

WordPress Light Poll plugin versions 1.0.0 and below suffer from multiple cross site request forgery vulnerabilities.

- [Link](#)

—

” “Tue, 13 Aug 2024

**WordPress PVN Auth Popup 1.0.0 Cross Site Scripting**

WordPress PVN Auth Popup plugin version 1.0.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 13 Aug 2024

**Giftora 1.0 Cross Site Request Forgery**

Giftora version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Tue, 13 Aug 2024

***Gas Agency Management 2022 Shell Upload***

Gas Agency Management version 2022 suffers from a remote shell upload vulnerability.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Thu, 15 Aug 2024

***ZDI-24-1151: Ivanti Avalanche WLAvalancheService Null Pointer Dereference Denial-of-Service Vulnerability***

- [Link](#)

—

” “Thu, 15 Aug 2024

***ZDI-24-1150: Ivanti Avalanche decodeToMap XML External Entity Processing Information Disclosure Vulnerability***

- [Link](#)

—

” “Thu, 15 Aug 2024

***ZDI-24-1149: Ivanti Avalanche deleteSkin Directory Traversal Arbitrary File Deletion Vulnerability***

- [Link](#)

—

” “Tue, 13 Aug 2024

***ZDI-24-1148: Microsoft Office PowerPoint PPTX File Parsing Use-After-Free Remote Code Execution Vulnerability***

- [Link](#)

—

” “Tue, 13 Aug 2024

***ZDI-24-1147: Microsoft Windows 10 WinREUpdateInstaller\_2401B\_amd64 Link Following Privilege Escalation Vulnerability***

- [Link](#)

—

” “Tue, 13 Aug 2024

***ZDI-24-1146: Microsoft Windows 10 WinREUpdateInstaller DLL Hijacking Local Privilege Escalati-***

**on Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1145: Microsoft Office Visio VSDX File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1144: Adobe Substance 3D Stager SKP File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1143: Adobe Dimension SKP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1142: Adobe Dimension SKP File Parsing Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1141: Adobe Dimension GLB File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1140: Adobe Dimension USD File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1139: Adobe Bridge AVI File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1138: Adobe Bridge JP2 File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1137: Adobe Bridge AVI File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1136: Adobe Acrobat Reader DC AcroForm Annotation Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1135: Adobe Acrobat Reader DC AcroForm Annotation Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1134: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1133: Adobe Acrobat Reader DC AcroForm Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1132: Adobe Acrobat Reader DC Annotation Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1131: Adobe Acrobat Reader DC Annotation Out-Of-Bounds Read Information Disclosure Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1130: Adobe Acrobat Reader DC Annotation Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1129: Magnet Forensics AXIOM Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1128: Samsung MagicInfo Server getFileFromMultipartFile Directory Traversal Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1127: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1126: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1125: Foxit PDF Reader AcroForm Use-After-Free Remote Code Execution Vulnerability**

- [Link](#)

—

” “Tue, 13 Aug 2024

**ZDI-24-1124: Foxit PDF Reader Doc Object Use-After-Free Information Disclosure Vulnerability**

- [Link](#)

—

” “Mon, 12 Aug 2024

**ZDI-24-1123: (Pwn2Own) QNAP TS-464 Netmgr Endpoint Command Injection Remote Code Execution Vulnerability**

- [Link](#)

—

”

## 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: (Aug)

Datum	Opfer	Land	Information
2024-08-13	District scolaire indépendant de Gadsden	[USA]	<a href="#">Link</a>
2024-08-12	Benson, Kearley & Associates Insurance Brokers Ltd.	[CAN]	<a href="#">Link</a>
2024-08-11	Université Paris-Saclay	[FRA]	<a href="#">Link</a>
2024-08-10	2Park	[NLD]	<a href="#">Link</a>
2024-08-09	Quálitás	[MEX]	<a href="#">Link</a>
2024-08-09	Schlatter Industries AG	[CHE]	<a href="#">Link</a>
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	<a href="#">Link</a>
2024-08-07	Killeen	[USA]	<a href="#">Link</a>
2024-08-06	Nilörn	[SWE]	<a href="#">Link</a>
2024-08-06	Sumter County Sheriff's Office	[USA]	<a href="#">Link</a>
2024-08-05	La ville de North Miami	[USA]	<a href="#">Link</a>
2024-08-05	McLaren Health Care	[USA]	<a href="#">Link</a>
2024-08-04	RMN-Grand Palais	[FRA]	<a href="#">Link</a>
2024-08-03	Xtrim	[ECU]	<a href="#">Link</a>
2024-08-02	Ihecs	[BEL]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-15	[www.isnart.it]	ransomhub	<a href="#">Link</a>
2024-08-15	[www.atwoodcherny.com]	ransomhub	<a href="#">Link</a>
2024-08-13	[Mill Creek Lumber]	play	<a href="#">Link</a>
2024-08-14	[Patterson Health Center]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-15	[www.prinsotel.com]	qilin	<a href="#">Link</a>
2024-08-15	[Seaway Manufacturing Corp.]	fog	<a href="#">Link</a>
2024-08-15	[FD S.R.L.]	ciphbit	<a href="#">Link</a>
2024-08-15	[The Pyle Group]	medusa	<a href="#">Link</a>
2024-08-15	[Zydus Pharmaceuticals]	meow	<a href="#">Link</a>
2024-08-15	[EPS Tech Ltd]	handala	<a href="#">Link</a>
2024-08-15	[MBS Radio]	metaencryptor	<a href="#">Link</a>
2024-08-15	[Liberty Resources]	rhysida	<a href="#">Link</a>
2024-08-15	[megatravel.com.mx]	darkvault	<a href="#">Link</a>
2024-08-14	[startaxi.com]	killsec	<a href="#">Link</a>
2024-08-14	[Boni]	akira	<a href="#">Link</a>
2024-08-14	[The Washington Times]	rhysida	<a href="#">Link</a>
2024-08-12	[Benson Kearley IFG - Insurance Brokers & Financial Advisors]	bianlian	<a href="#">Link</a>
2024-08-14	[Texas Centers for Infectious Disease Associates]	bianlian	<a href="#">Link</a>
2024-08-14	[Thompson Davis & Co]	bianlian	<a href="#">Link</a>
2024-08-14	[police.praca.gov.pl]	ransomhub	<a href="#">Link</a>
2024-08-14	[mmtransport.com]	dAn0n	<a href="#">Link</a>
2024-08-14	[Riley Pope & Laney]	cicada3301	<a href="#">Link</a>
2024-08-13	[hugwi.ch]	helldown	<a href="#">Link</a>
2024-08-13	[Forrec]	blacksuit	<a href="#">Link</a>
2024-08-13	[American Contract Systems]	meow	<a href="#">Link</a>
2024-08-13	[Element Food Solutions]	meow	<a href="#">Link</a>
2024-08-13	[Aerotech Solutions]	meow	<a href="#">Link</a>
2024-08-13	[E-Z UP]	meow	<a href="#">Link</a>
2024-08-13	[Safefood]	meow	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-13	[Gaston Fence]	meow	<a href="#">Link</a>
2024-08-13	[Parker Development Company]	play	<a href="#">Link</a>
2024-08-13	[Air International Thermal Systems]	play	<a href="#">Link</a>
2024-08-13	[Adina Design]	play	<a href="#">Link</a>
2024-08-13	[CinemaTech]	play	<a href="#">Link</a>
2024-08-13	[Erie Meats]	play	<a href="#">Link</a>
2024-08-13	[M??? ???k ?????]	play	<a href="#">Link</a>
2024-08-13	[SCHLATTNER.de]	helldown	<a href="#">Link</a>
2024-08-13	[deganis.fr]	helldown	<a href="#">Link</a>
2024-08-13	[The White Center Community Development Association]	rhysida	<a href="#">Link</a>
2024-08-13	[lenmed.co.za]	darkvault	<a href="#">Link</a>
2024-08-13	[gpf.org.za]	darkvault	<a href="#">Link</a>
2024-08-13	[Banner and Associates]	trinity	<a href="#">Link</a>
2024-08-13	[Southwest Family Medicine Associates]	bianlian	<a href="#">Link</a>
2024-08-13	[glazkov.co.il]	darkvault	<a href="#">Link</a>
2024-08-05	[XPERT Business Solutions GmbH]	helldown	<a href="#">Link</a>
2024-08-05	[MyFreightWorld]	helldown	<a href="#">Link</a>
2024-08-09	[cbmm.org]	helldown	<a href="#">Link</a>
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	<a href="#">Link</a>
2024-08-11	[briju.pl]	helldown	<a href="#">Link</a>
2024-08-11	[vindix.pl]	helldown	<a href="#">Link</a>
2024-08-11	[Albatros S.r.l.]	helldown	<a href="#">Link</a>
2024-08-12	[NetOne]	hunters	<a href="#">Link</a>
2024-08-12	[fabamaq.com]	BrainCipher	<a href="#">Link</a>
2024-08-12	[cyceron.fr]	BrainCipher	<a href="#">Link</a>
2024-08-12	[bedford.k12.oh.us]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-12	[Warwick Hotels and Resorts]	lynx	<a href="#">Link</a>
2024-08-12	[VVS-Eksperten]	cicada3301	<a href="#">Link</a>
2024-08-12	[Brookshire Dental]	qilin	<a href="#">Link</a>
2024-08-07	[Alvan Blanch Development]	lynx	<a href="#">Link</a>
2024-08-11	[parkerdevco.com]	dispossessor	<a href="#">Link</a>
2024-08-11	[naturalcuriosities.com]	ransomhub	<a href="#">Link</a>
2024-08-11	[TelPro]	play	<a href="#">Link</a>
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	<a href="#">Link</a>
2024-08-11	[Amco Metal Industrial Corporation]	qilin	<a href="#">Link</a>
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	<a href="#">Link</a>
2024-08-11	[Moser Wealth Advisors]	rhysida	<a href="#">Link</a>
2024-08-09	[alliuminteriors.co.nz]	ransomhub	<a href="#">Link</a>
2024-08-11	[robertshvac.com]	abyss	<a href="#">Link</a>
2024-08-11	[dmmerch.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[luisoliveras.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[legacypas.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[allweatheraa.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[soprema.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[exol-lubricants.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[fremontschools.net]	lockbit3	<a href="#">Link</a>
2024-08-11	[acdcexpress.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[clinatezza.com.pe]	lockbit3	<a href="#">Link</a>
2024-08-11	[divaris.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[sullivansteelservice.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[johnllowery.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[qespavements.com]	lockbit3	<a href="#">Link</a>
2024-08-11	[emanic.net]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-11	[Hanon Systems]	hunters	<a href="#">Link</a>
2024-08-10	[kronospublic.com]	lockbit3	<a href="#">Link</a>
2024-08-10	[Brontoo Technology Solutions]	ransomexx	<a href="#">Link</a>
2024-08-07	[Cydcor]	dragonforce	<a href="#">Link</a>
2024-08-09	[Credible Group]	play	<a href="#">Link</a>
2024-08-09	[Nilorngruppen AB]	play	<a href="#">Link</a>
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	<a href="#">Link</a>
2024-08-09	[Anniversary Holding Company]	bianlian	<a href="#">Link</a>
2024-08-09	[GCA Global Cargo Alliance]	bianlian	<a href="#">Link</a>
2024-08-09	[Majestic Metals]	bianlian	<a href="#">Link</a>
2024-08-09	[dhcgrp.com]	ransomhub	<a href="#">Link</a>
2024-08-05	[Boombah Inc.]	incransom	<a href="#">Link</a>
2024-08-09	[www.dunnsolutions.com]	dAn0n	<a href="#">Link</a>
2024-08-09	[Sumter County Sheriff]	rhysida	<a href="#">Link</a>
2024-08-06	[pierrediamonds.com.au]	ransomhub	<a href="#">Link</a>
2024-08-08	[golfoy.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[inv-dar.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[icarasia.com]	killsec	<a href="#">Link</a>
2024-08-08	[rationalenterprise.com]	ransomhub	<a href="#">Link</a>
2024-08-02	[modernceramics.com]	ransomhub	<a href="#">Link</a>
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	<a href="#">Link</a>
2024-08-08	[tibaitservices.com]	cactus	<a href="#">Link</a>
2024-08-08	[mihlfeld.com]	cactus	<a href="#">Link</a>
2024-08-08	[Horizon View Medical Center]	everest	<a href="#">Link</a>
2024-08-08	[comoferta.com]	darkvault	<a href="#">Link</a>
2024-08-08	[NIDEC CORPORATION]	everest	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-08	[mercadomineiro.com.br]	darkvault	<a href="#">Link</a>
2024-08-07	[hudsoncivil.com.au]	ransomhub	<a href="#">Link</a>
2024-08-07	[www.jgsummit.com.ph]	ransomhub	<a href="#">Link</a>
2024-08-07	[Bayhealth Hospital]	rhysida	<a href="#">Link</a>
2024-08-07	[amplicon.com]	ransomhub	<a href="#">Link</a>
2024-08-06	[infotexim.pe]	ransomhub	<a href="#">Link</a>
2024-08-07	[suandco.com]	madliberator	<a href="#">Link</a>
2024-08-07	[Anderson Oil & Gas]	hunters	<a href="#">Link</a>
2024-08-07	[bonatra.com]	killsec	<a href="#">Link</a>
2024-08-07	[FatBoy Cellular]	meow	<a href="#">Link</a>
2024-08-07	[KLA]	meow	<a href="#">Link</a>
2024-08-07	[HUD User]	meow	<a href="#">Link</a>
2024-08-06	[msprocuradores.es]	madliberator	<a href="#">Link</a>
2024-08-06	[www.carri.com]	alphalocker	<a href="#">Link</a>
2024-08-06	[www.consortzioinnova.it]	alphalocker	<a href="#">Link</a>
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	<a href="#">Link</a>
2024-08-06	[biw-burger.de]	alphalocker	<a href="#">Link</a>
2024-08-06	[www.sobha.com]	ransomhub	<a href="#">Link</a>
2024-08-06	[Alternate Energy]	play	<a href="#">Link</a>
2024-08-06	[True Blue Environmental]	play	<a href="#">Link</a>
2024-08-06	[Granit Design]	play	<a href="#">Link</a>
2024-08-06	[KinetX]	play	<a href="#">Link</a>
2024-08-06	[Omni Family Health]	hunters	<a href="#">Link</a>
2024-08-06	[IOI Corporation Berhad]	fog	<a href="#">Link</a>
2024-08-06	[Ziba Design]	fog	<a href="#">Link</a>
2024-08-06	[Casco Antiguo]	hunters	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-06	[Fractalia Group]	hunters	<a href="#">Link</a>
2024-08-06	[Banx Systems]	meow	<a href="#">Link</a>
2024-08-05	[Silipos]	cicada3301	<a href="#">Link</a>
2024-08-04	[kierlcpa.com]	lockbit3	<a href="#">Link</a>
2024-08-05	[Square One Coating Systems]	cicada3301	<a href="#">Link</a>
2024-08-05	[Hi-P International]	fog	<a href="#">Link</a>
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	<a href="#">Link</a>
2024-08-05	[HP Distribution]	incransom	<a href="#">Link</a>
2024-08-05	[exco-solutions.com]	cactus	<a href="#">Link</a>
2024-08-05	[Maryville Academy]	rhysida	<a href="#">Link</a>
2024-08-04	[notariusze.waw.pl]	killsec	<a href="#">Link</a>
2024-08-04	[Ranney School]	rhysida	<a href="#">Link</a>
2024-08-03	[nursing.com]	ransomexx	<a href="#">Link</a>
2024-08-03	[Bettis Asphalt]	blacksuit	<a href="#">Link</a>
2024-08-03	[fcl.crs]	lockbit3	<a href="#">Link</a>
2024-08-03	[CPA Tax Solutions]	meow	<a href="#">Link</a>
2024-08-03	[LRN]	hunters	<a href="#">Link</a>
2024-08-03	[aikenhousing.org]	blacksuit	<a href="#">Link</a>
2024-08-02	[David E Shambach Architect]	dragonforce	<a href="#">Link</a>
2024-08-02	[Hayes Beer Distributing]	dragonforce	<a href="#">Link</a>
2024-08-02	[Jangho Group]	hunters	<a href="#">Link</a>
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	<a href="#">Link</a>
2024-08-02	[retaildatallc.com]	ransomhub	<a href="#">Link</a>
2024-08-02	[WPG Holdings]	meow	<a href="#">Link</a>
2024-08-02	[National Beverage]	meow	<a href="#">Link</a>
2024-08-02	[PeoplesHR]	meow	<a href="#">Link</a>
2024-08-02	[Dometic Group]	meow	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-02	[Remitano]	meow	<a href="#">Link</a>
2024-08-02	[Premier Equities]	meow	<a href="#">Link</a>
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	<a href="#">Link</a>
2024-08-02	[q-cells.de]	abyss	<a href="#">Link</a>
2024-08-02	[coinbv.nl]	madliberator	<a href="#">Link</a>
2024-08-01	[Valley Bulk]	cicada3301	<a href="#">Link</a>
2024-08-01	[ENEA Italy]	hunters	<a href="#">Link</a>
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	<a href="#">Link</a>
2024-08-01	[effinghamschools.com]	ransomhub	<a href="#">Link</a>
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	<a href="#">Link</a>
2024-08-01	[Adorna & Guzman Dentistry]	monti	<a href="#">Link</a>
2024-08-01	[Camp Susque]	medusa	<a href="#">Link</a>
2024-08-01	[Ali Gohar]	medusa	<a href="#">Link</a>
2024-08-01	[acsi.org]	blacksuit	<a href="#">Link</a>
2024-08-01	[County Linen UK]	dispossessor	<a href="#">Link</a>
2024-08-01	[TNT Materials tnt-materials.com/]	dispossessor	<a href="#">Link</a>
2024-08-01	[Peñoles]	akira	<a href="#">Link</a>
2024-08-01	[dahlvalve.com]	cactus	<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.