

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240820



## 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>18</b>
5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus. . . .	18
<b>6 Cyberangriffe: (Aug)</b>	<b>19</b>
<b>7 Ransomware-Erpressungen: (Aug)</b>	<b>19</b>
<b>8 Quellen</b>	<b>28</b>
8.1 Quellenverzeichnis . . . . .	28
<b>9 Impressum</b>	<b>30</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

#### ***Server mit IBM App Connect Enterprise können nach Attacke abstürzen***

IBMs Integrationssoftware App Connect Enterprise ist über eine Sicherheitslücke angreifbar. Ein Sicherheitspatch steht zum Download bereit.

- [Link](#)

—

#### ***Sicherheitspatch: Angreifer können Dovecot-Mail-Server lahmlegen***

Dovecot-IMAP-Server können sich an präparierten E-Mails verschlucken und in einem DoS-Zustand enden.

- [Link](#)

—

#### ***Jetzt patchen! Schadcode-Attacken auf Solarwinds Web Help Desk beobachtet***

Angreifer nutzen derzeit eine kritische Schwachstelle Solarwinds Web Help Desk aus. Ein Sicherheitspatch ist verfügbar, kann aber mitunter für Probleme sorgen.

- [Link](#)

—

#### ***Serverüberwachung: OpenBMC-Lücke bringt Systeme in Gefahr***

Eine kritische Sicherheitslücke in der OpenBMC-Firmware gefährdet Computer. Ein Sicherheitspatch ist verfügbar.

- [Link](#)

—

#### ***Zoom schützt Anwendungen unter Linux, macOS und Windows vor möglichen Attacken***

Es sind wichtige Sicherheitsupdates für unter anderem Zoom Workplace und Rooms Client erschienen.

- [Link](#)

—

#### ***Sicherheitsupdates F5: Angreifer können unbefugt auf BIG-IP-Appliances zugreifen***

Mehrere Sicherheitslücken ermöglichen Attacken auf BIG-IP Next Central Manager und BIG-IP Next SPK.

- [Link](#)

—

#### ***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](#)

---

### 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	0.990720000	<a href="#">Link</a>
CVE-2023-5360	0.902780000	0.988750000	<a href="#">Link</a>
CVE-2023-52251	0.944080000	0.992550000	<a href="#">Link</a>
CVE-2023-4966	0.971280000	0.998310000	<a href="#">Link</a>
CVE-2023-49103	0.962110000	0.995600000	<a href="#">Link</a>
CVE-2023-48795	0.965330000	0.996440000	<a href="#">Link</a>
CVE-2023-47246	0.959010000	0.995010000	<a href="#">Link</a>
CVE-2023-46805	0.937250000	0.991710000	<a href="#">Link</a>
CVE-2023-46747	0.972820000	0.998880000	<a href="#">Link</a>
CVE-2023-46604	0.961790000	0.995540000	<a href="#">Link</a>
CVE-2023-4542	0.928310000	0.990810000	<a href="#">Link</a>
CVE-2023-43208	0.972240000	0.998620000	<a href="#">Link</a>
CVE-2023-43177	0.964550000	0.996170000	<a href="#">Link</a>
CVE-2023-42793	0.970220000	0.997890000	<a href="#">Link</a>
CVE-2023-41265	0.911110000	0.989290000	<a href="#">Link</a>
CVE-2023-39143	0.939130000	0.991970000	<a href="#">Link</a>
CVE-2023-38646	0.906610000	0.988980000	<a href="#">Link</a>
CVE-2023-38205	0.953670000	0.994110000	<a href="#">Link</a>
CVE-2023-38203	0.966410000	0.996730000	<a href="#">Link</a>
CVE-2023-38146	0.920720000	0.989940000	<a href="#">Link</a>
CVE-2023-38035	0.974920000	0.999810000	<a href="#">Link</a>
CVE-2023-36845	0.966270000	0.996690000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-3519	0.965340000	0.996450000	<a href="#">Link</a>
CVE-2023-35082	0.966130000	0.996640000	<a href="#">Link</a>
CVE-2023-35078	0.970440000	0.997950000	<a href="#">Link</a>
CVE-2023-34993	0.973130000	0.999020000	<a href="#">Link</a>
CVE-2023-34960	0.928290000	0.990810000	<a href="#">Link</a>
CVE-2023-34634	0.925130000	0.990480000	<a href="#">Link</a>
CVE-2023-34468	0.906650000	0.988990000	<a href="#">Link</a>
CVE-2023-34362	0.971000000	0.998200000	<a href="#">Link</a>
CVE-2023-34039	0.947770000	0.993080000	<a href="#">Link</a>
CVE-2023-3368	0.937150000	0.991690000	<a href="#">Link</a>
CVE-2023-33246	0.972040000	0.998510000	<a href="#">Link</a>
CVE-2023-32315	0.970220000	0.997890000	<a href="#">Link</a>
CVE-2023-30625	0.953800000	0.994120000	<a href="#">Link</a>
CVE-2023-30013	0.962380000	0.995660000	<a href="#">Link</a>
CVE-2023-29300	0.968930000	0.997440000	<a href="#">Link</a>
CVE-2023-29298	0.947600000	0.993060000	<a href="#">Link</a>
CVE-2023-28432	0.911820000	0.989330000	<a href="#">Link</a>
CVE-2023-28343	0.942300000	0.992340000	<a href="#">Link</a>
CVE-2023-28121	0.909500000	0.989150000	<a href="#">Link</a>
CVE-2023-27524	0.970600000	0.998020000	<a href="#">Link</a>
CVE-2023-27372	0.972120000	0.998580000	<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	0.996400000	<a href="#">Link</a>
CVE-2023-26035	0.967360000	0.997000000	<a href="#">Link</a>
CVE-2023-25717	0.954250000	0.994220000	<a href="#">Link</a>
CVE-2023-25194	0.967920000	0.997160000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963960000	0.996030000	<a href="#">Link</a>
CVE-2023-24489	0.973870000	0.999300000	<a href="#">Link</a>
CVE-2023-23752	0.956380000	0.994610000	<a href="#">Link</a>
CVE-2023-23333	0.962300000	0.995640000	<a href="#">Link</a>
CVE-2023-22527	0.968290000	0.997250000	<a href="#">Link</a>
CVE-2023-22518	0.965970000	0.996590000	<a href="#">Link</a>
CVE-2023-22515	0.973250000	0.999060000	<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	0.964660000	0.996190000	<a href="#">Link</a>
CVE-2023-0669	0.969760000	0.997730000	<a href="#">Link</a>

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

Mon, 19 Aug 2024

#### **[NEU] [hoch] Moodle: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um Code auszuführen, bestimmte administrative Aufgaben durchzuführen, Informationen preiszugeben, Daten zu manipulieren, Sicherheitsmechanismen zu umgehen, Cross-Site-Scripting-Angriffe durchzuführen und eine nicht näher spezifizierte Wirkung zu erzielen.

- [Link](#)

—

Mon, 19 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](#)

—

Mon, 19 Aug 2024



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

Ein entfernter, anonymer 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](#)

—

Mon, 19 Aug 2024

**[NEU] [hoch] Kubernetes: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Kubernetes im “ingress-nginx controller” ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Mon, 19 Aug 2024

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

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

- [Link](#)

—

Mon, 19 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](#)

—

Mon, 19 Aug 2024

**[UPDATE] [hoch] QT: Schwachstelle ermöglicht Offenlegung von Informationen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in QT ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Mon, 19 Aug 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Django ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Mon, 19 Aug 2024

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

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

- [Link](#)

—

Mon, 19 Aug 2024

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

Ein entfernter anonymmer 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](#)

—

Fri, 16 Aug 2024

**[UPDATE] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen**

Ein entfernter, anonymmer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Fri, 16 Aug 2024

**[UPDATE] [hoch] Foxit PDF Editor: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Foxit PDF Editor ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- [Link](#)

—

Fri, 16 Aug 2024

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

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

- [Link](#)

—

Fri, 16 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

***[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] [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 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] 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](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/19/2024	[Amazon Linux 2023 : iwl100-firmware, iwl105-firmware, iwl135-firmware (ALAS2023-2024-706)]	high
8/19/2024	[Amazon Linux 2023 : p7zip, p7zip-plugins (ALAS2023-2024-705)]	high
8/19/2024	[Amazon Linux 2023 : postgresql15, postgresql15-contrib, postgresql15-llvmjit (ALAS2023-2024-702)]	high
8/19/2024	[Oracle Linux 9 : python3.12-setuptools (ELSA-2024-5533)]	high
8/19/2024	[RHEL 8 : kpatch-patch-4_18_0-372_87_1 and kpatch-patch-4_18_0-372_91_1 (RHSA-2024:5582)]	high
8/19/2024	[RHEL 9 : libreoffice (RHSA-2024:5584)]	high
8/19/2024	[RHEL 9 : libreoffice (RHSA-2024:5583)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : sssd (EulerOS-SA-2024-2149)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : mod_http2 (EulerOS-SA-2024-2143)]	high

Datum	Schwachstelle	Bewertung
8/19/2024	[EulerOS Virtualization 2.10.0 : glibc (EulerOS-SA-2024-2117)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : python-idna (EulerOS-SA-2024-2146)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : kernel (EulerOS-SA-2024-2120)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : systemd (EulerOS-SA-2024-2130)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : expat (EulerOS-SA-2024-2136)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : libxml2 (EulerOS-SA-2024-2122)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : systemd (EulerOS-SA-2024-2150)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : sssd (EulerOS-SA-2024-2129)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : httpd (EulerOS-SA-2024-2119)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : python-idna (EulerOS-SA-2024-2126)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : curl (EulerOS-SA-2024-2134)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : expat (EulerOS-SA-2024-2116)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : kernel (EulerOS-SA-2024-2140)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : glibc (EulerOS-SA-2024-2137)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : less (EulerOS-SA-2024-2141)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : httpd (EulerOS-SA-2024-2139)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : mod_http2 (EulerOS-SA-2024-2123)]	high

Datum	Schwachstelle	Bewertung
8/19/2024	[EulerOS Virtualization 2.10.0 : curl (EulerOS-SA-2024-2114)]	high
8/19/2024	[EulerOS Virtualization 2.10.0 : less (EulerOS-SA-2024-2121)]	high
8/19/2024	[EulerOS Virtualization 2.10.1 : libxml2 (EulerOS-SA-2024-2142)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Mon, 19 Aug 2024

#### ***Ewon Cosy+ / Talk2M Remote Access Solution Improper Authentication***

During account assignment in the Talk2M platform, a Cosy+ device generates and sends a certificate signing request (CSR) to the back end. This CSR is then signed by the manufacturer and used for OpenVPN authentication by the device afterward. Since the common name (CN) of the certificate is specified by the device and used in order to assign the OpenVPN session to the corresponding Talk2M account, an attacker with root access to a Cosy+ device is able to manipulate the CSR and get correctly signed certificates for foreign devices.

- [Link](#)

—

” “Mon, 19 Aug 2024

#### ***Dovecot IMAP Server 2.2 / 2.3 Denial Of Service***

Dovecot IMAP server versions 2.2 and 2.3 suffer from denial of service and resource exhaustion vulnerabilities.

- [Link](#)

—

” “Mon, 19 Aug 2024

#### ***Dovecot IMAP Server 2.2 / 2.3 Missing Rate Limiting***

Dovecot IMAP server versions 2.2 and 2.3 have an issue where a large number of address headers (From, To, Cc, Bcc, etc.) becomes excessively CPU intensive. With 100k header lines CPU usage is already 12 seconds, and in a production environment we observed 500k header lines taking 18 minutes to parse. Since this can be triggered by external actors sending emails to a victim, this is a security issue.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Ewon Cosy+ Hardcoded Key***

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. Due to the use of a hardcoded cryptographic key, an attacker is able to decrypt encrypted data and retrieve sensitive information.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Ewon Cosy+ Command Injection***

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. Due to improper neutralization of parameters read from a user-controlled configuration file, an authenticated attacker is able to inject and execute OS commands on the device.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Ewon Cosy+ Password Disclosure***

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. The credentials used for the basic authentication against the web interface of Cosy+ are stored in the cookie "credentials" after a successful login. An attacker with access to a victim's browser is able to retrieve the administrative password of Cosy+.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Ewon Cosy+ Improper Neutralization / Cross Site Scripting***

The Ewon Cosy+ is a VPN gateway used for remote access and maintenance in industrial environments. If login against the FTP service of the Cosy+ fails, the submitted username is saved in a log. This log is included in the Cosy+ web interface without neutralizing the content. As a result, an unauthenticated attacker is able to inject HTML/JavaScript code via the username of an FTP login attempt.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Lawyer CMS 1.6 Insecure Settings***

Lawyer CMS version 1.6 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Karya Online Shopping Portal 2.0 SQL Injection***

Karya Online Shopping Portal version 2.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Mon, 19 Aug 2024

***JobSeeker CMS 1.5 Insecure Settings***

JobSeeker CMS version 1.5 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Jobs Finder System 1.0 SQL Injection***

Jobs Finder System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Human Resource Management System 2024 1.0 Insecure Settings***

Human Resource Management System 2024 version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Hotel Management System 1.0 Cross Site Request Forgery***

Hotel Management System version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Bhojon Restaurant Management System 3.0 Insecure Settings***

Bhojon Restaurant Management System version 3.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Mon, 19 Aug 2024

***Accounting Journal Management System 1.0 Cross Site Request Forgery***

Accounting Journal Management System version 1.0 suffers from a cross site request forgery vulnerability.

- [Link](#)

—

” “Fri, 16 Aug 2024



**WordPress Shield Security 20.0.5 Cross Site Scripting**

WordPress Shield Security plugin versions 20.0.5 and below cross site scripting exploit that adds an administrative user.

- [Link](#)

—

” “Fri, 16 Aug 2024

**Build Your Own Botnet 2.0.0 Remote Code Execution**

Build Your Own Botnet (BYOB) version 2.0.0 exploit that works by spoofing an agent callback to overwrite the sqlite database and bypass authentication and exploiting an authenticated command injection in the payload builder page.

- [Link](#)

—

” “Fri, 16 Aug 2024

**Insurance 1.2 Insecure Settings**

Insurance version 1.2 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Fri, 16 Aug 2024

**Human Resource Management System 2024 1.0 SQL Injection**

Human Resource Management System 2024 version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Fri, 16 Aug 2024

**Hotel Management System 1.0 SQL Injection**

Hotel Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Fri, 16 Aug 2024

**Hotel Booking System 1.0 Shell Upload**

Hotel Booking System version 1.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Fri, 16 Aug 2024

**Home Owners Collection Management System 1.0 Insecure Settings**

Home Owners Collection Management System version 1.0 suffers from an ignored default credential vulnerability.

- [Link](#)

—

” “Fri, 16 Aug 2024

***Giftora 1.0 Cross Site Scripting***

Giftora version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 16 Aug 2024

***Bhojon Restaurant Management System 3.0 Insecure Direct Object Reference***

Bhojon Restaurant Management System version 3.0 suffers from an insecure direct object reference vulnerability.

- [Link](#)

—

” “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](#)

—

”

## **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: (Aug)

Datum	Opfer	Land	Information
2024-08-18	Lagoon	[NCL]	<a href="#">Link</a>
2024-08-16	Contarina	[ITA]	<a href="#">Link</a>
2024-08-14	Flint	[USA]	<a href="#">Link</a>
2024-08-13	District scolaire indépendant de Gadsden	[USA]	<a href="#">Link</a>
2024-08-13	IPNext	[ARG]	<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>
2024-08-11	AutoCanada	[CAN]	<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>
2024-08-08	Evolution Mining	[AUS]	<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
2024-08-19	[OSG.COM]	ransomhub	<a href="#">Link</a>
2024-08-14	[imobesidade.com.br]	ransomhub	<a href="#">Link</a>
2024-08-19	[Waynesboro Nurseries]	rhysida	<a href="#">Link</a>
2024-08-19	[The Transit Authority of Northern Kentucky (TANK)]	akira	<a href="#">Link</a>
2024-08-19	[Khonaysser]	helldown	<a href="#">Link</a>
2024-08-11	[Jangho Group]	ransomhouse	<a href="#">Link</a>
2024-08-19	[Certified Transmission]	meow	<a href="#">Link</a>
2024-08-19	[Bandier]	blacksuit	<a href="#">Link</a>
2024-08-18	[ccsdschools.com]	ransomhub	<a href="#">Link</a>
2024-08-19	[Ferraro Group]	hunters	<a href="#">Link</a>
2024-08-18	[kbo]	helldown	<a href="#">Link</a>
2024-08-18	[Mohawk Valley Cardiology PC]	bianlian	<a href="#">Link</a>
2024-08-18	[PBC Companies]	bianlian	<a href="#">Link</a>
2024-08-17	[Yang Enterprises]	dragonforce	<a href="#">Link</a>
2024-08-17	[Carver Companies]	dragonforce	<a href="#">Link</a>
2024-08-17	[J&J Network Engineering]	dragonforce	<a href="#">Link</a>
2024-08-18	[PER4MANCE]	dragonforce	<a href="#">Link</a>
2024-08-18	[SMK Ingenieurbüro]	dragonforce	<a href="#">Link</a>
2024-08-18	[Cosmetic Dental Group]	trinity	<a href="#">Link</a>
2024-08-17	[TELECO]	stormous	<a href="#">Link</a>
2024-08-17	[peoplewell.com]	darkvault	<a href="#">Link</a>
2024-08-17	[aerworldwide.com]	lockbit3	<a href="#">Link</a>
2024-08-17	[awsag.com]	madliberator	<a href="#">Link</a>
2024-08-17	[www.albynhousing.org.uk]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.lennartsfors.com]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.allanmcneill.co.nz]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-08-17	[www.martinswood.herts.sch.uk]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.gmchc.org]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.regentcaravans.com.au]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.netconfig.co.za]	ransomhub	<a href="#">Link</a>
2024-08-17	[www.manotherm.ie]	ransomhub	<a href="#">Link</a>
2024-08-17	[tiendasmacuto.com]	BrainCipher	<a href="#">Link</a>
2024-08-15	[nrcollecties.nl]	ransomhub	<a href="#">Link</a>
2024-08-17	[Zyxel.eu]	helldown	<a href="#">Link</a>
2024-08-10	[www.wmwmeyer.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[www.vinakom.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[Keios Development Consulting]	ciphbit	<a href="#">Link</a>
2024-08-16	[Lennartsfors AB]	meow	<a href="#">Link</a>
2024-08-16	[Rostance Edwards]	meow	<a href="#">Link</a>
2024-08-16	[SuperDrob S.A.]	hunters	<a href="#">Link</a>
2024-08-16	[Sterling Rope]	rhysida	<a href="#">Link</a>
2024-08-16	[www.patelco.org]	ransomhub	<a href="#">Link</a>
2024-08-14	[ljglaw.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[Hiesmayr Haustechnik]	qilin	<a href="#">Link</a>
2024-08-15	[www.aaconsultinc.com]	ransomhub	<a href="#">Link</a>
2024-08-16	[promises2kids.org]	qilin	<a href="#">Link</a>
2024-08-16	[BTS Biogas]	hunters	<a href="#">Link</a>
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>
2024-08-15	[www.prinsotel.com]	qilin	<a href="#">Link</a>
2024-08-15	[Seaway Manufacturing Corp.]	fog	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-08-13	[Gaston Fence]	meow	<a href="#">Link</a>
2024-08-13	[Parker Development Company]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-08-12	[Warwick Hotels and Resorts]	lynx	<a href="#">Link</a>
2024-08-12	[VVS-Eksperten]	cicada3301	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
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	[legacycpas.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>
2024-08-11	[Hanon Systems]	hunters	<a href="#">Link</a>
2024-08-10	[kronospublic.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2024-08-08	[mercadomineiro.com.br]	darkvault	<a href="#">Link</a>
2024-08-07	[hudsoncivil.com.au]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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.consorziainnova.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>
2024-08-06	[Fractalia Group]	hunters	<a href="#">Link</a>
2024-08-06	[Banx Systems]	meow	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[retaildata LLC.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>
2024-08-02	[Remitano]	meow	<a href="#">Link</a>
2024-08-02	[Premier Equities]	meow	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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.