# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241224

# Inhaltsverzeichnis

# 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

***Kritische Sicherheitslücken bedrohen Sophos-Firewalls***

Es sind wichtige Sicherheitsupdates für Firewalls von Sophos erschienen. Mit den Standardeinstellungen installieren sie sich automatisch.

- Link

—

***Fortinet Wireless Manager: Informationen zu kritischer Lücke zurückgehalten***

Angreifer konnten Fortinet Wireless Manager attackieren und Admins-Sessions kapern. Das Netzwerkmanagementool war über mehrere Monate verwundbar.

- Link

—

***Kritische Lücke in BeyondTrust Privileged Remote Access und Remote Support***

In aktuellen Versionen von BeyondTrust Privileged Remote Access und Remote Support haben die Entwickler eine gefährliche Schwachstelle geschlossen.

- Link

—

***Windows-Sicherheitslösung Trend Micro Apex One als Einfallstor für Angreifer***

Angreifer können an mehreren Sicherheitslücken in Trend Micro Apex One ansetzen. Sicherheitsupdates sind verfügbar.

- Link

—

***Jetzt patchen! Angreifer nutzen kritische Sicherheitslücke in Apache Struts aus***

Die Uploadfunktion von Apache Struts ist fehlerhaft und Angreifer können Schadcode hochladen. Sicherheitsforscher warnen vor Attacken.

- Link

—

***Foxit PDF Editor und Reader: Attacken über präparierte PDF-Dateien möglich***

PDF-Anwendungen von Foxit sind unter macOS und Windows verwundbar. Sicherheitsupdates stehen bereit.

- Link

—

***CyberPanel: Angreifer können Schadcode einschleusen***

In der Server-Verwaltungssoftware CyberPanel wurden zwei Schwachstellen entdeckt. Sie erlauben Angreifern das Einschleusen beliebigen Codes.

- Link

—

***DevSecOps-Plattform Gitlab: Accountübernahme möglich***

Sicherheitsupdates für Gitlab beugen unter anderem unberechtigte Zugriffe und DoS-Attacken vor.

- Link

—

***Sicherheitsupdates: Dell schließt Lücken in PCs, Treibern und Zubehör***

Angreifer können mehrere Sicherheitslücken in Dells Hard- und Software ausnutzen. Nun sind Sicherheitspatches erschienen.

- Link

—

***Sicherheitspatch: Angreifer können über TeamViewer-Lücke Windows-Dateien löschen***

In der aktuellen Version einer Komponente des Fernzugriffsclients TeamViewer für Windows haben die Entwickler eine Schwachstelle geschlossen.

- Link

—

# 3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

## 3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden.

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-7028 | 0.916790000 | 0.991560000 | Link |
| CVE-2023-6895 | 0.929940000 | 0.992690000 | Link |
| CVE-2023-6553 | 0.955740000 | 0.995580000 | Link |
| CVE-2023-6019 | 0.942220000 | 0.993880000 | Link |
| CVE-2023-6018 | 0.929560000 | 0.992660000 | Link |
| CVE-2023-52251 | 0.946770000 | 0.994360000 | Link |
| CVE-2023-4966 | 0.954120000 | 0.995370000 | Link |
| CVE-2023-49103 | 0.950490000 | 0.994900000 | Link |
| CVE-2023-48795 | 0.946090000 | 0.994280000 | Link |
| CVE-2023-47246 | 0.961710000 | 0.996560000 | Link |
| CVE-2023-46805 | 0.964050000 | 0.997090000 | Link |
| CVE-2023-46747 | 0.973480000 | 0.999530000 | Link |
| CVE-2023-46604 | 0.971630000 | 0.998970000 | Link |
| CVE-2023-4542 | 0.923100000 | 0.992100000 | Link |
| CVE-2023-43208 | 0.975000000 | 0.999890000 | Link |
| CVE-2023-43177 | 0.966560000 | 0.997650000 | Link |
| CVE-2023-42793 | 0.974860000 | 0.999860000 | Link |
| CVE-2023-4220 | 0.955830000 | 0.995600000 | Link |
| CVE-2023-39143 | 0.922430000 | 0.992050000 | Link |
| CVE-2023-38035 | 0.971600000 | 0.998960000 | Link |
| CVE-2023-35813 | 0.919220000 | 0.991780000 | Link |
| CVE-2023-3519 | 0.964130000 | 0.997120000 | Link |
| CVE-2023-35082 | 0.961850000 | 0.996620000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-35078 | 0.967920000 | 0.997970000 | Link |
| CVE-2023-34993 | 0.968280000 | 0.998050000 | Link |
| CVE-2023-34362 | 0.970610000 | 0.998680000 | Link |
| CVE-2023-34105 | 0.923620000 | 0.992150000 | Link |
| CVE-2023-34039 | 0.956980000 | 0.995750000 | Link |
| CVE-2023-3368 | 0.941220000 | 0.993770000 | Link |
| CVE-2023-33246 | 0.973380000 | 0.999510000 | Link |
| CVE-2023-32707 | 0.900600000 | 0.990540000 | Link |
| CVE-2023-32315 | 0.970610000 | 0.998690000 | Link |
| CVE-2023-32235 | 0.921560000 | 0.991980000 | Link |
| CVE-2023-30625 | 0.945900000 | 0.994240000 | Link |
| CVE-2023-30013 | 0.967560000 | 0.997860000 | Link |
| CVE-2023-29298 | 0.971300000 | 0.998890000 | Link |
| CVE-2023-28432 | 0.934340000 | 0.993090000 | Link |
| CVE-2023-28343 | 0.966300000 | 0.997580000 | Link |
| CVE-2023-28121 | 0.913860000 | 0.991350000 | Link |
| CVE-2023-27524 | 0.972940000 | 0.999360000 | Link |
| CVE-2023-27372 | 0.973390000 | 0.999520000 | Link |
| CVE-2023-27350 | 0.968700000 | 0.998150000 | Link |
| CVE-2023-26469 | 0.947200000 | 0.994420000 | Link |
| CVE-2023-26035 | 0.969170000 | 0.998300000 | Link |
| CVE-2023-25717 | 0.953520000 | 0.995290000 | Link |
| CVE-2023-25194 | 0.965880000 | 0.997480000 | Link |
| CVE-2023-2479 | 0.965350000 | 0.997380000 | Link |
| CVE-2023-24489 | 0.972380000 | 0.999200000 | Link |
| CVE-2023-23752 | 0.938470000 | 0.993480000 | Link |
| CVE-2023-23333 | 0.965180000 | 0.997340000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-22527 | 0.970640000 | 0.998700000 | Link |
| CVE-2023-22518 | 0.970030000 | 0.998490000 | Link |
| CVE-2023-22515 | 0.971440000 | 0.998930000 | Link |
| CVE-2023-20887 | 0.972150000 | 0.999140000 | Link |
| CVE-2023-1671 | 0.956590000 | 0.995710000 | Link |
| CVE-2023-0669 | 0.969800000 | 0.998440000 | Link |
| CVE-2023-0315 | 0.912680000 | 0.991280000 | Link |
| CVE-2023-0297 | 0.948870000 | 0.994630000 | Link |

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

Mon, 23 Dec 2024

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

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreiferkann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und und die Sicherheitsmaßnahmen zu umgehen.

- Link

—

Mon, 23 Dec 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Mon, 23 Dec 2024

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

Ein Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows Server und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, um Sicherheitsmechanismen zu umgehen, um einen Denial of Service Zustand herbeizuführen und um beliebigen Code

auszuführen.

- Link

—

Mon, 23 Dec 2024

***[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen***

Ein Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows Server und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, vertrauliche Informationen preiszugeben und einen Spoofing-Angriff durchzuführen.

- Link

—

Mon, 23 Dec 2024

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

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Mon, 23 Dec 2024

***[UPDATE] [hoch] Gitea: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Gitea ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 23 Dec 2024

***[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen ermöglichen Codeausführung***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 23 Dec 2024

***[NEU] [hoch] Apache Tomcat: Schwachstelle ermöglicht Codeausführung***

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

- Link

—

Mon, 23 Dec 2024

***[NEU] [hoch] Webmin: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode***

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Webmin ausnutzen, um beliebigen Programmcode mit Root-Rechten auszuführen.

- Link

—

Fri, 20 Dec 2024

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und einen Spoofing-Angriff durchzuführen.

- Link

—

Fri, 20 Dec 2024

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

Ein entfernter, anonymer, authentifizierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen und einen Denial of Service Zustand herzustellen.

- Link

—

Fri, 20 Dec 2024

***[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen***

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Fri, 20 Dec 2024

***[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle in unbound***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um eine laufende Instanz zu manipulieren, Informationen offenzulegen oder einen Denial-of-Service auszulösen.

- Link

—

Fri, 20 Dec 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Fri, 20 Dec 2024

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

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

- Link

—

Fri, 20 Dec 2024

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

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

- Link

—

Fri, 20 Dec 2024

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

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

- Link

—

Fri, 20 Dec 2024

***[UPDATE] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 20 Dec 2024

***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service***

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder nicht näher beschriebene Auswirkungen zu erzielen.

- Link

—

Fri, 20 Dec 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen

Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren oder vertrauliche Informationen preiszugeben.
- Link
—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 12/23/2024 | [Apache Tomcat 9.0.0-M1 < 9.0.98 Multiple Vulnerabilities] | critical |
| 12/23/2024 | [Fortra GoAnywhere Managed File Transfer (MFT) < 7.4.2 Path Traversal (CVE-2024-25156)] | critical |
| 12/23/2024 | [Fortra FileCatalyst Workflow Directory Traversal (CVE-2024-25153) (Version Check)] | critical |
| 12/23/2024 | [Fedora 40 : prometheus-podman-exporter (2024-f2a4ffc1ff)] | critical |
| 12/23/2024 | [Fedora 41 : prometheus-podman-exporter (2024-8d1b3f4466)] | critical |
| 12/23/2024 | [Amazon Linux 2 : flatpak (ALAS-2024-2712)] | critical |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-088)] | critical |
| 12/23/2024 | [AlmaLinux 9 : skopeo (ALSA-2024:11217)] | high |
| 12/23/2024 | [AlmaLinux 9 : containernetworking-plugins (ALSA-2024:11216)] | high |
| 12/23/2024 | [Oracle Linux 7 : postgresql (ELSA-2024-10882)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-057)] | high |
| 12/23/2024 | [Amazon Linux 2 : java-1.8.0-openjdk (ALAS-2024-2720)] | high |
| 12/23/2024 | [Amazon Linux 2 : NetworkManager-libreswan (ALAS-2024-2703)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-089)] | high |

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 12/23/2024 | [Amazon Linux 2 : postgresql (ALASPOSTGRESQL13-2024-008)] | high |
| 12/23/2024 | [Amazon Linux 2 : libsoup (ALAS-2024-2705)] | high |
| 12/23/2024 | [Amazon Linux 2 : ghostscript (ALAS-2024-2708)] | high |
| 12/23/2024 | [Amazon Linux 2 : expat (ALAS-2024-2710)] | high |
| 12/23/2024 | [Amazon Linux 2 : ruby (ALAS-2024-2706)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-075)] | high |
| 12/23/2024 | [Amazon Linux 2 : zziplib (ALAS-2024-2713)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-059)] | high |
| 12/23/2024 | [Amazon Linux 2 : libpq (ALASPOSTGRESQL14-2024-015)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-074)] | high |
| 12/23/2024 | [Amazon Linux 2 : libxml2 (ALAS-2024-2717)] | high |
| 12/23/2024 | [Amazon Linux 2 : postgresql (ALASPOSTGRESQL14-2024-014)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-076)] | high |
| 12/23/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-058)] | high |
| 12/23/2024 | [Amazon Linux 2 : java-11-openjdk (ALASJAVA-OPENJDK11-2024-010)] | high |
| 12/23/2024 | [Amazon Linux 2 : edk2 (ALAS-2024-2722)] | high |
| 12/23/2024 | [Amazon Linux 2 : xstream (ALAS-2024-2707)] | high |
| 12/23/2024 | [Amazon Linux 2 : dovecot (ALAS-2024-2719)] | high |
| 12/23/2024 | [Debian dla-4002 : intel-microcode - security update] | high |

# 4 Aktiv ausgenutzte Sicherheitslücken

## 4.1 Exploits der letzten 5 Tage

“Tue, 03 Dec 2024

***Acronis Cyber Protect/Backup Remote Code Execution***

The Acronis Cyber Protect appliance, in its default configuration, allows the anonymous registration of new protect/backup agents on new endpoints. This API endpoint also generates bearer tokens which the agent then uses to authenticate to the appliance. As the management web console is running on the same port as the API for the agents, this bearer token is also valid for any actions on the web console. This allows an attacker with network access to the appliance to start the registration of a new agent, retrieve a bearer token that provides admin access to the available functions in the web console. The web console contains multiple possibilities to execute arbitrary commands on both the agents (e.g., via PreCommands for a backup) and also the appliance (e.g., via a Validation job on the agent of the appliance). These options can easily be set with the provided bearer token, which leads to a complete compromise of all agents and the appliance itself.

- Link

—

” “Tue, 03 Dec 2024

***Fortinet FortiManager Unauthenticated Remote Code Execution***

This Metasploit module exploits a missing authentication vulnerability affecting FortiManager and FortiManager Cloud devices to achieve unauthenticated RCE with root privileges. The vulnerable FortiManager versions are 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, and 6.2.0 through 6.2.12. The vulnerable FortiManager Cloud versions are 7.4.1 through 7.4.4, 7.2.1 through 7.2.7, 7.0.1 through 7.0.12, and 6.4 (all versions).

- Link

—

” “Tue, 03 Dec 2024

***Asterisk AMI Originate Authenticated Remote Code Execution***

On Asterisk, prior to versions 18.24.2, 20.9.2, and 21.4.2 and certified-asterisk versions 18.9-cert11 and 20.7-cert2, an AMI user with write=originate may change all configuration files in the /etc/asterisk/ directory. Writing a new extension can be created which performs a system command to achieve RCE as the asterisk service user (typically asterisk). Default parking lot in FreePBX is called ”Default lot” on the website interface, however its actually parkedcalls. Tested against Asterisk 19.8.0 and 18.16.0 on Freepbx SNG7-PBX16-64bit-2302-1.

- Link

—

” “Mon, 02 Dec 2024

***Omada Identity Cross Site Scripting***

Omada Identity versions prior to 15U1 and 14.14 hotfix #309 suffer from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 02 Dec 2024

***Siemens Unlocked JTAG Interface / Buffer Overflow***

Various Siemens products suffer from vulnerabilities. There is an unlocked JTAG Interface for Zynq-7000 on SM-2558 and a buffer overflow on the webserver of the SM-2558, CP-2016, and CP-2019 systems.

- Link

—

” “Mon, 02 Dec 2024

***ABB Cylon Aspect 3.08.00 fileSystemUpdate.php File Upload / Denial Of Service***

ABB Cylon Aspect version 3.08.00 suffers from a vulnerability in the fileSystemUpdate.php endpoint of the ABB BEMS controller due to improper handling of uploaded files. The endpoint lacks restrictions on file size and type, allowing attackers to upload excessively large or malicious files. This flaw could be exploited to cause denial of service (DoS) attacks, memory leaks, or buffer overflows, potentially leading to system crashes or further compromise.

- Link

—

” “Mon, 02 Dec 2024

***ABB Cylon Aspect 3.08.01 mstpstatus.php Information Disclosure***

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose various BACnet MS/TP statistics running on the device.

- Link

—

” “Mon, 02 Dec 2024

***ABB Cylon Aspect 3.08.01 diagLateThread.php Information Disclosure***

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated information disclosure vulnerability. An unauthorized attacker can reference the affected page and disclose various protocol thread information running on the device.

- Link

—

” “Mon, 02 Dec 2024

***AppleAVD AV1_Syntax::Parse_Header Out-Of-Bounds Reads***

AppleAVD has an issue where a large OBU size in AV1_Syntax::Parse_Header reading can lead to out-of-bounds reads.

- Link

—

” “Mon, 02 Dec 2024

***AppleAVD AV1_Syntax::f Out-Of-Bounds Reads***

AppleAVD has an issue in AV1_Syntax::f leading to out-of-bounds reads.

- Link

—

” “Mon, 02 Dec 2024

***AppleAVD AV1_Syntax::Parse_Header Integer Underflow / Out-Of-Bounds Reads***

AppleAVD has an integer underflow in AV1_Syntax::Parse_Header that can lead to out-of-bounds reads.

- Link

—

” “Mon, 02 Dec 2024

***Simple Chat System 1.0 Cross Site Scripting***

Simple Chat System version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 02 Dec 2024

***Russian FSB Cross Site Scripting***

The Russian FSB appears to suffer from a cross site scripting vulnerability. The researchers who discovered it have reported it multiple times to them.

- Link

—

” “Mon, 02 Dec 2024

***Laravel 11.0 Cross Site Scripting***

Laravel version 11.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 02 Dec 2024

***Nvidia GeForce 11.0.1.163 Unquoted Service Path***

Nvidia GeForce version 11.0.1.163 suffers from an unquoted service path vulnerability.

- Link

—

” “Mon, 02 Dec 2024

***Intelligent Security System SecurOS Enterprise 11 Unquoted Service Path***

Intelligent Security System SecurOS Enterprise version 11 suffers from an unquoted service path vulnerability.

- Link

—

” “Wed, 27 Nov 2024

***ABB Cylon Aspect 3.08.01 vstatConfigurationDownload.php Configuration Download***

ABB Cylon Aspect version 3.08.01 suffers from an unauthenticated configuration download vul-

nerability. This can be exploited to download the CSV DB that contains the configuration mappings information via the VMobileImportExportServlet by directly calling the vstatConfigurationDownload.php script.

- Link

—

” “Wed, 27 Nov 2024

***Akuvox Smart Intercom/Doorphone ServicesHTTPAPI Improper Access Control***

The Akuvox Smart Intercom/Doorphone suffers from an insecure service API access control. The vulnerability in ServicesHTTPAPI endpoint allows users with ”User” privileges to modify API access settings and configurations. This improper access control permits privilege escalation, enabling unauthorized access to administrative functionalities. Exploitation of this issue could compromise system integrity and lead to unauthorized system modifications.

- Link

—

” “Fri, 22 Nov 2024

***CUPS IPP Attributes LAN Remote Code Execution***

This Metasploit module exploits vulnerabilities in OpenPrinting CUPS, which is running by default on most Linux distributions. The vulnerabilities allow an attacker on the LAN to advertise a malicious printer that triggers remote code execution when a victim sends a print job to the malicious printer. Successful exploitation requires user interaction, but no CUPS services need to be reachable via accessible ports. Code execution occurs in the context of the lp user. Affected versions are cups-browsed less than or equal to 2.0.1, libcupsfilters versions 2.1b1 and below, libppd versions 2.1b1 and below, and cups-filters versions 2.0.1 and below.

- Link

—

” “Fri, 22 Nov 2024

***ProjectSend R1605 Unauthenticated Remote Code Execution***

This Metasploit module exploits an improper authorization vulnerability in ProjectSend versions r1295 through r1605. The vulnerability allows an unauthenticated attacker to obtain remote code execution by enabling user registration, disabling the whitelist of allowed file extensions, and uploading a malicious PHP file to the server.

- Link

—

” “Fri, 22 Nov 2024

***needrestart Local Privilege Escalation***

Qualys discovered that needrestart suffers from multiple local privilege escalation vulnerabilities that allow for root access from an unprivileged user.

- Link

—

” “Fri, 22 Nov 2024

***fronsetia 1.1 Cross Site Scripting***

fronsetia version 1.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Fri, 22 Nov 2024

***fronsetia 1.1 XML Injection***

fronsetia version 1.1 suffers from an XML external entity injection vulnerability.

- Link

—

” “Fri, 22 Nov 2024

***PowerVR psProcessHandleBase Reuse***

PowerVR has an issue where PVRSRVAcquireProcessHandleBase() can cause psProcessHandleBase reuse when PIDs are reused.

- Link

—

” “Fri, 22 Nov 2024

***Linux 6.6 Race Condition***

A security-relevant race between mremap() and THP code has been discovered. Reaching the buggy code typically requires the ability to create unprivileged namespaces. The bug leads to installing physical address 0 as a page table, which is likely exploitable in several ways: For example, triggering the bug in multiple processes can probably lead to unintended page table sharing, which probably can lead to stale TLB entries pointing to freed pages.

- Link

—

”

## 4.2 0-Days der letzten 5 Tage

“Fri, 20 Dec 2024

***ZDI-24-1726: Linux Kernel ksmbd TCP Connection Memory Exhaustion Denial-of-Service Vulnerability***

- Link

—

” “Fri, 20 Dec 2024

***ZDI-24-1725: Webmin CGI Command Injection Remote Code Execution Vulnerability***

- Link

—

” “Fri, 20 Dec 2024

***ZDI-24-1724: (0Day) Delta Electronics DRASimuCAD STP File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Fri, 20 Dec 2024

***ZDI-24-1723: (0Day) Delta Electronics DRASimuCAD ICS File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Fri, 20 Dec 2024

***ZDI-24-1722: (0Day) Delta Electronics DRASimuCAD STP File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Fri, 20 Dec 2024

***ZDI-24-1721: Delta Electronics DTM Soft BIN File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability***

- Link

—

”

# 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Gehackt via Nachbar... oder die Palo Alto.


Zum Youtube Video

## 6 Cyberangriffe: (Dez)

| Datum | Opfer | Land | Information |
|---|---|---|---|
| 2024-12-18 | Christopher Newport University | [USA] | Link |
| 2024-12-15 | Arsoé de Soual | [FRA] | Link |
| 2024-12-12 | Taylor Regional Hospital | [USA] | Link |
| 2024-12-11 | Avril | [CAN] | Link |
| 2024-12-11 | Vincit | [FIN] | Link |
| 2024-12-09 | Muswellbrook Shire Council | [AUS] | Link |
| 2024-12-09 | Wood County | [USA] | Link |
| 2024-12-08 | Societatea Energetica Electrica S.A. | [GBR] | Link |
| 2024-12-08 | Fundación Arturo López Pérez (FALP) | [CHL] | Link |
| 2024-12-08 | Ecritel | [FRA] | Link |
| 2024-12-07 | Vidymed | [CHE] | Link |
| 2024-12-06 | Compass Communications | [NZL] | Link |
| 2024-12-04 | Fournisseur de services responsable de la collecte des amendes en retard au Manitoba | [CAN] | Link |
| 2024-12-02 | Pembina Trails School Division | [CAN] | Link |
| 2024-12-02 | Wayne-Westland Community Schools | [USA] | Link |
| 2024-12-02 | ITO EN (North America) INC. | [USA] | Link |
| 2024-12-02 | Marietta City Schools | [USA] | Link |
| 2024-12-01 | PIH Health | [USA] | Link |
| 2024-12-01 | Klinikum Ingolstadt | [DEU] | Link |

## 7 Ransomware-Erpressungen: (Dez)

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-24 | [Baker Tilly Morrison Murray] | sarcoma | Link |
| 2024-12-24 | [Kern Services] | sarcoma | Link |
| 2024-12-21 | [Farrar & Ball] | lynx | Link |
| 2024-12-24 | [itc.gov.ae with 1K !] | funksec | Link |
| 2024-12-24 | [egyptair.com 5 sell] | funksec | Link |
| 2024-12-24 | [asjp.cerist.dz sell] | funksec | Link |
| 2024-12-23 | [acwlaw.com] | lockbit3 | Link |
| 2024-12-23 | [www.globelink.com.au] | qilin | Link |
| 2024-12-23 | [klingler-installationen-gmbh] | qilin | Link |
| 2024-12-23 | [Flamco] | qilin | Link |
| 2024-12-18 | [intellinet-es.com] | ransomhub | Link |
| 2024-12-23 | [www.semfin.com] | ransomhub | Link |
| 2024-12-16 | [www.mccoyglobal.com] | ransomhub | Link |
| 2024-12-23 | [awimc.com] | cactus | Link |
| 2024-12-23 | [tsebrakes.com] | lockbit3 | Link |
| 2024-12-23 | [marmon-herrington.com] | lockbit3 | Link |
| 2024-12-23 | [egyptair.com 5 with 10K !] | funksec | Link |
| 2024-12-23 | [galatachemicals.com] | cactus | Link |
| 2024-12-23 | [n4telecom.com.br] | apt73 | Link |
| 2024-12-23 | [linebank.co.id] | apt73 | Link |
| 2024-12-23 | [9fsfalcons.org] | lockbit3 | Link |
| 2024-12-13 | [Rhode Island Department of Humain Services] | BrainCipher | Link |
| 2024-12-23 | [SmartLynx Airlines SIA] | hunters | Link |
| 2024-12-23 | [kfar-yona.muni.il] | funksec | Link |
| 2024-12-23 | [RODS Surveying (rods.cc)] | fog | Link |
| 2024-12-23 | [Albion College] | medusa | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-23 | [asiapacfish.org] | funksec | Link |
| 2024-12-23 | [10M israeli data for sell] | funksec | Link |
| 2024-12-23 | [Forum Architecture & Interior Design (forumarchitecture.com)] | fog | Link |
| 2024-12-23 | [Gallade Chemical (galladechem.com)] | fog | Link |
| 2024-12-23 | [Industria e Comercio Jolitex Ltda (jolitex.com)] | fog | Link |
| 2024-12-23 | [Billet Precision] | akira | Link |
| 2024-12-23 | [ptcky.com] | cactus | Link |
| 2024-12-23 | [Billet Precision (billetprecision.ca)] | akira | Link |
| 2024-12-12 | [adveo.com] | cactus | Link |
| 2024-12-22 | [STIIIZY Pre-Christmas publication] | everest | Link |
| 2024-12-22 | [visualsystemas.com.ar] | funksec | Link |
| 2024-12-22 | [casarom.com.ar] | funksec | Link |
| 2024-12-22 | [ibericar] | monti | Link |
| 2024-12-22 | [gtsportcarrental.com] | funksec | Link |
| 2024-12-22 | [Sicoob] | 8base | Link |
| 2024-12-21 | [Blome International] | killsec | Link |
| 2024-12-21 | [BRIGHT BOLT ENTERPRISES INC] | killsec | Link |
| 2024-12-21 | [Casa Juarez Restaurant Supply Co] | killsec | Link |
| 2024-12-21 | [Davis Products Company Inc] | killsec | Link |
| 2024-12-21 | [Economy Restaurant Equipment And Supply Company] | killsec | Link |
| 2024-12-21 | [GAMKA SALES CO. INC] | killsec | Link |
| 2024-12-21 | [Greater Michigan Distributors] | killsec | Link |
| 2024-12-21 | [GPM Lawn Sprinkler Supply] | killsec | Link |
| 2024-12-21 | [Greene Supply Company] | killsec | Link |
| 2024-12-21 | [Hammons Supply Company] | killsec | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-21 | [J AND S Electrical And Lighting Supply LLC] | killsec | Link |
| 2024-12-21 | [LAMERS ENTERPRISE INC] | killsec | Link |
| 2024-12-21 | [Langford Tool And Drill Co] | killsec | Link |
| 2024-12-21 | [McCally Tool and Supply] | killsec | Link |
| 2024-12-21 | [berkotfoods.com] | abyss | Link |
| 2024-12-21 | [Abrasive Supply Corporation] | killsec | Link |
| 2024-12-21 | [Albert Paper Company] | killsec | Link |
| 2024-12-21 | [Allied Packing And Rubber Inc] | killsec | Link |
| 2024-12-21 | [Avana Electrotek] | killsec | Link |
| 2024-12-21 | [Badger Popcorn And Concession Supply Company] | killsec | Link |
| 2024-12-21 | [news.gdi.gov.kh] | funksec | Link |
| 2024-12-21 | [fusioncharts.com] | funksec | Link |
| 2024-12-01 | [Grupo Bébécar] | 8base | Link |
| 2024-12-01 | [CLARKE CENTRE D'IMAGERIE MEDICALE INC.] | 8base | Link |
| 2024-12-01 | [GNK Golf] | 8base | Link |
| 2024-12-21 | [carsbeat.com] | funksec | Link |
| 2024-12-03 | [www.marietta-city.org] | ransomhub | Link |
| 2024-12-21 | [www.groupe-setcar.com.tn] | ransomhub | Link |
| 2024-12-14 | [gilariver.org] | ransomhub | Link |
| 2024-12-20 | [Accolent ERP Software] | killsec | Link |
| 2024-12-20 | [Genie Healthcare] | everest | Link |
| 2024-12-20 | [Izmocars] | everest | Link |
| 2024-12-20 | [Frameworks] | cicada3301 | Link |
| 2024-12-20 | [ndc.energy.mn] | funksec | Link |
| 2024-12-20 | [tabocas.com.br] | ransomhub | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-20 | [Schenkelberg - Die Medienstrategen (schenkelberg-druck.de)] | fog | Link |
| 2024-12-20 | [Village Community School (vcsnyc.org)] | fog | Link |
| 2024-12-20 | [Circle Electric (circleelectric.com)] | fog | Link |
| 2024-12-19 | [Broker Educational Sales & Training] | medusa | Link |
| 2024-12-20 | [PT Pertamina] | killsec | Link |
| 2024-12-20 | [Howell Township Public Schools (howell.k12.nj.us)] | fog | Link |
| 2024-12-20 | [EP Holdings (epholdingsinc.com)] | fog | Link |
| 2024-12-20 | [Khalil Center] | killsec | Link |
| 2024-12-20 | [Water Utilities Corporation] | killsec | Link |
| 2024-12-20 | [Fmp.gob.pe] | cloak | Link |
| 2024-12-19 | [JRT Automatisation] | spacebears | Link |
| 2024-12-18 | [planetgroup.co.il] | ransomhub | Link |
| 2024-12-13 | [www.tekni-plex.com] | ransomhub | Link |
| 2024-12-19 | [Compliance Solutions Inc] | qilin | Link |
| 2024-12-19 | [Krispy Kreme] | play | Link |
| 2024-12-20 | [austinsfs.com.au] | kairos | Link |
| 2024-12-20 | [City of Noblesville] | interlock | Link |
| 2024-12-20 | [HostingExpress.com.mx] | funksec | Link |
| 2024-12-20 | [sklepbaterie.pl] | funksec | Link |
| 2024-12-19 | [Jet Edge (jetedgewaterjets.com)] | fog | Link |
| 2024-12-19 | [Energy Capital Credit Union (eccu.net)] | fog | Link |
| 2024-12-20 | [federalbank.co.in] | apt73 | Link |
| 2024-12-19 | [Jared Beschel and Associates] | akira | Link |
| 2024-12-19 | [Hide-A-Way Lake Club] | akira | Link |
| 2024-12-19 | [Leyman Manufacturing] | akira | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-19 | [agti.eng.br] | funksec | Link |
| 2024-12-19 | [web.vaips.cl] | funksec | Link |
| 2024-12-19 | [EMPRESARIA.COM] | clop | Link |
| 2024-12-19 | [IMSPLGROUP.COM] | clop | Link |
| 2024-12-08 | [CK Technology Group] | cicada3301 | Link |
| 2024-12-15 | [Concession Peugeot] | cicada3301 | Link |
| 2024-12-19 | [bataviacontainer.com] | abyss | Link |
| 2024-12-12 | [Banner Day Camp] | lynx | Link |
| 2024-12-18 | [Astaphans] | hunters | Link |
| 2024-12-18 | [Microvision] | hunters | Link |
| 2024-12-18 | [Trev Deeley Motorcycles] | hunters | Link |
| 2024-12-18 | [Development Bank of Jamaica] | hunters | Link |
| 2024-12-18 | [Archetype Group] | hunters | Link |
| 2024-12-18 | [National Atomic Energy Commission] | moneymessage | Link |
| 2024-12-18 | [Smith Tank & Steel (smith-tank.com)] | lynx | Link |
| 2024-12-18 | [Verosa LLC] | killsec | Link |
| 2024-12-18 | [chixking.ca] | funksec | Link |
| 2024-12-18 | [flybase.org] | funksec | Link |
| 2024-12-18 | [Nathan American Academy] | funksec | Link |
| 2024-12-18 | [robertfinaleeditions] | funksec | Link |
| 2024-12-18 | [seaislerealty.com] | funksec | Link |
| 2024-12-18 | [abd-ong.org] | funksec | Link |
| 2024-12-18 | [Vroninks Ricker Weyts & Sacre- Notaires (notassoc.be)] | fog | Link |
| 2024-12-18 | [Reliance Connects (relianceconnects.com)] | fog | Link |
| 2024-12-18 | [Archie Cochrane Ford] | akira | Link |
| 2024-12-18 | [Cottrell Fletcher & Cottrell P.C.] | bianlian | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-18 | [Giordano, DelCollo, Werb & Gagne, LLC.] | bianlian | Link |
| 2024-12-18 | [OL Products] | akira | Link |
| 2024-12-18 | [fote.com] | blackbasta | Link |
| 2024-12-18 | [bender.de] | blackbasta | Link |
| 2024-12-18 | [valveworksusa.com] | blackbasta | Link |
| 2024-12-18 | [wikov.com] | blackbasta | Link |
| 2024-12-18 | [Skopos] | akira | Link |
| 2024-12-18 | [activedynamics.com] | blackbasta | Link |
| 2024-12-18 | [bathfitter.com] | blackbasta | Link |
| 2024-12-18 | [grimaldialliance.com] | blackbasta | Link |
| 2024-12-18 | [medion.com] | blackbasta | Link |
| 2024-12-18 | [bri.co.id] | apt73 | Link |
| 2024-12-18 | [Freightlinerof Savannah] | akira | Link |
| 2024-12-18 | [Black Oak Casino Resort] | akira | Link |
| 2024-12-18 | [Fullmer Construction] | akira | Link |
| 2024-12-18 | [massdevelopment.com] | cactus | Link |
| 2024-12-18 | [furmanos.com] | blackbasta | Link |
| 2024-12-18 | [Modern Dental Group Limited] | BrainCipher | Link |
| 2024-12-18 | [Avstar Fuel Systems] | rhysida | Link |
| 2024-12-17 | [Groupe-fimar] | bluebox | Link |
| 2024-12-17 | [Tharisa] | termite | Link |
| 2024-12-17 | [ibram.org.br] | funksec | Link |
| 2024-12-17 | [dinamalar.com] | funksec | Link |
| 2024-12-14 | [choicemg.com] | ransomhub | Link |
| 2024-12-14 | [medisecure.com.au] | ransomhub | Link |
| 2024-12-14 | [redknee.com] | ransomhub | Link |
| 2024-12-14 | [nbleisuretrust.org] | ransomhub | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-17 | [kuritaamerica.com] | threeam | Link |
| 2024-12-16 | [Billaud] | qilin | Link |
| 2024-12-17 | [Kilgore Industries] | nitrogen | Link |
| 2024-12-17 | [A Geradora] | akira | Link |
| 2024-12-17 | [A Beautiful Pools Inc] | nitrogen | Link |
| 2024-12-17 | [Fireproof Contractors Inc] | nitrogen | Link |
| 2024-12-17 | [SpeedLine Solutions (speedlinesolutions.com)] | fog | Link |
| 2024-12-17 | [Toscano Law] | akira | Link |
| 2024-12-17 | [Polskie Wydawnictwo Muzyczne] | akira | Link |
| 2024-12-17 | [Ouro Verde (ouroverde.net.br)] | fog | Link |
| 2024-12-17 | [Heritage Bank] | interlock | Link |
| 2024-12-17 | [rtdc.gov.mn] | funksec | Link |
| 2024-12-17 | [pbos.gov.pk] | funksec | Link |
| 2024-12-14 | [FINN] | dragonforce | Link |
| 2024-12-14 | [Williams Tank Lines] | dragonforce | Link |
| 2024-12-14 | [Engineered Tower Solutions] | dragonforce | Link |
| 2024-12-14 | [Marine Floats] | dragonforce | Link |
| 2024-12-08 | [Ecritel] | hunters | Link |
| 2024-12-17 | [Total Patient Care LLC;A Sensitive Touch Home Health;Alphastar Home Health Care;Heart of T] | everest | Link |
| 2024-12-17 | [Artistic Family Dental;Value Dental Center;Sparkling Smiles Family Dentistry] | everest | Link |
| 2024-12-16 | [phantomsecurity.ca] | dragonransomw | Link |
| 2024-12-16 | [Joshua Grading & Excavating] | play | Link |
| 2024-12-16 | [South Plains Implement] | play | Link |
| 2024-12-16 | [Chemitex SA Information] | play | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-11 | [favbet] | qilin | Link |
| 2024-12-16 | [Hatfield Consultants] | play | Link |
| 2024-12-16 | [Lanigan Ryan] | play | Link |
| 2024-12-16 | [Welker] | play | Link |
| 2024-12-16 | [eisenhowerlaw.com] | kairos | Link |
| 2024-12-16 | [bushandburchett.com] | ransomhub | Link |
| 2024-12-16 | [SWDAKOTAH.COM] | ransomhub | Link |
| 2024-12-11 | [CM Buck & Associates] | lynx | Link |
| 2024-12-16 | [Cognity (cognity.gr)] | fog | Link |
| 2024-12-16 | [Waverley Christian College (wcc.vic.edu.au)] | fog | Link |
| 2024-12-16 | [amlakparto.ir] | dragonransomw | Link |
| 2024-12-16 | [www.prixet.com] | apt73 | Link |
| 2024-12-16 | [Time Machine Inc] | akira | Link |
| 2024-12-16 | [baseisapis.it] | argonauts | Link |
| 2024-12-16 | [National Air Vibrator] | akira | Link |
| 2024-12-16 | [Simmtech Co., Ltd.] | underground | Link |
| 2024-12-16 | [Great Plains Bank] | akira | Link |
| 2024-12-16 | [Rob Levine & Associates] | akira | Link |
| 2024-12-16 | [Diferencial Energia] | akira | Link |
| 2024-12-16 | [Acumen Group] | ElDorado | Link |
| 2024-12-16 | [LaSen] | ElDorado | Link |
| 2024-12-12 | [www.aflak.com.sa] | ransomhub | Link |
| 2024-12-16 | [scania.pl] | ransomhub | Link |
| 2024-12-16 | [GNS Cloud] | handala | Link |
| 2024-12-10 | [Biodimed] | stormous | Link |
| 2024-12-15 | [JSSR Options Co., Ltd. (JSSR)] | killsec | Link |
| 2024-12-15 | [Tumeny Payments Limited] | killsec | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-15 | [akobdc.com] | funksec | Link |
| 2024-12-15 | [indianaerospaceand] | funksec | Link |
| 2024-12-15 | [arkajainuniver] | funksec | Link |
| 2024-12-15 | [gstpam.org] | funksec | Link |
| 2024-12-15 | [rangiamb.org.in] | funksec | Link |
| 2024-12-15 | [pathsalatc.org.in] | funksec | Link |
| 2024-12-15 | [ekitistate.gov.ng] | funksec | Link |
| 2024-12-12 | [Westfield Fire Department] | medusa | Link |
| 2024-12-12 | [North Los Angeles County Regional Center] | medusa | Link |
| 2024-12-13 | [Clarkson Insurance Group] | medusa | Link |
| 2024-12-03 | [www.whiteleafent.net] | dragonransomware | Link |
| 2024-12-04 | [starlinkvietnam.vn] | dragonransomw | Link |
| 2024-12-05 | [www.beikelogistics.com] | dragonransomware | Link |
| 2024-12-05 | [logikaservicios.cl] | dragonransomw | Link |
| 2024-12-05 | [stleasing.tj] | dragonransomware | Link |
| 2024-12-05 | [hinodes.in] | dragonransomw | Link |
| 2024-12-06 | [oakenglish.com] | dragonransomware | Link |
| 2024-12-06 | [cafunesol.in] | dragonransomw | Link |
| 2024-12-06 | [www.srishtisoft.com] | dragonransomware | Link |
| 2024-12-06 | [eosspartners.com] | dragonransomw | Link |
| 2024-12-06 | [ssfirm.com.sa] | dragonransomware | Link |
| 2024-12-06 | [k-boss.net] | dragonransomw | Link |
| 2024-12-06 | [tekryse.com] | dragonransomware | Link |
| 2024-12-08 | [parkaire.net] | dragonransomw | Link |
| 2024-12-10 | [www.infoer.com.ar] | dragonransomware | Link |
| 2024-12-12 | [eye-ed.com] | dragonransomw | Link |
| 2024-12-12 | [tg777.pub] | dragonransomware | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-12 | [timesexpress.net] | dragonransomw | Link |
| 2024-12-12 | [kpr-rm.com] | dragonransomware | Link |
| 2024-12-13 | [shoor.cc] | dragonransomw | Link |
| 2024-12-13 | [pid.co.zw] | dragonransomware | Link |
| 2024-12-14 | [Midland Turbo] | ElDorado | Link |
| 2024-12-14 | [First Baptist Church] | ElDorado | Link |
| 2024-12-14 | [Kandelaar Electrotechniek] | ElDorado | Link |
| 2024-12-14 | [Light Speed Design] | ElDorado | Link |
| 2024-12-14 | [American Computer Estimating Inc] | bianlian | Link |
| 2024-12-14 | [MedRevenu Inc] | bianlian | Link |
| 2024-12-14 | [Mid Florida Primary Care] | bianlian | Link |
| 2024-12-14 | [zetech.ac.ke] | funksec | Link |
| 2024-12-14 | [maxprofit.mcode.me] | funksec | Link |
| 2024-12-14 | [skopje.gov.mk] | funksec | Link |
| 2024-12-03 | [muswellbrook.nsw.gov.au] | safepay | Link |
| 2024-12-13 | [tekni-plex.com] | ransomhub | Link |
| 2024-12-13 | [www.hashem-contracting.com] | ransomhub | Link |
| 2024-12-13 | [aneticaid.com] | kairos | Link |
| 2024-12-13 | [tcpm.com] | kairos | Link |
| 2024-12-13 | [archlou.org] | kairos | Link |
| 2024-12-13 | [Kazyon] | moneymessage | Link |
| 2024-12-13 | [António Belém & António Gonçalves] | ciphbit | Link |
| 2024-12-13 | [lamundialdeseguros] | funksec | Link |
| 2024-12-13 | [bee-insurance.com] | funksec | Link |
| 2024-12-13 | [lamundialdeseguros.com] | funksec | Link |
| 2024-12-13 | [An independent private assets manager] | akira | Link |
| 2024-12-13 | [Luxor Capital Group] | akira | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-13 | [fuse.io] | funksec | Link |
| 2024-12-13 | [lakhipurmb.org.in] | funksec | Link |
| 2024-12-13 | [Myhealthcarebilling] | everest | Link |
| 2024-12-12 | [Sigarth] | play | Link |
| 2024-12-12 | [Long Beach Convention Center] | play | Link |
| 2024-12-12 | [Maxus Group] | play | Link |
| 2024-12-12 | [SBW] | play | Link |
| 2024-12-12 | [Sunline] | play | Link |
| 2024-12-10 | [Talascend] | lynx | Link |
| 2024-12-12 | [Artemis Holding] | play | Link |
| 2024-12-12 | [Arnott] | play | Link |
| 2024-12-12 | [Goins Law] | lynx | Link |
| 2024-12-05 | [Gills Onions] | lynx | Link |
| 2024-12-12 | [Wintergreen Learning Materials] | hunters | Link |
| 2024-12-12 | [AFD] | hunters | Link |
| 2024-12-04 | [GBC] | lynx | Link |
| 2024-12-12 | [Southern Acids] | hunters | Link |
| 2024-12-09 | [recope.go.cr] | ransomhub | Link |
| 2024-12-12 | [Estar Seguros, S.A.] | BrainCipher | Link |
| 2024-12-12 | [Cristal y Lavisa S.A. de C.V.] | BrainCipher | Link |
| 2024-12-12 | [Brasilmad] | sarcoma | Link |
| 2024-12-05 | [Watsonville Community Hospital] | termite | Link |
| 2024-12-11 | [Locke Solutions , LLC] | nitrogen | Link |
| 2024-12-11 | [CW Lighting, LLC] | nitrogen | Link |
| 2024-12-11 | [Compass Communications] | raworld | Link |
| 2024-12-11 | [Interforos Casting] | killsec | Link |
| 2024-12-11 | [Sarah Car Care] | everest | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-11 | [Primary Plus] | qilin | Link |
| 2024-12-11 | [AC Technical Systems] | qilin | Link |
| 2024-12-11 | [Bianco Brain & Spine] | qilin | Link |
| 2024-12-11 | [Tejas Office Products, Inc.] | nitrogen | Link |
| 2024-12-11 | [quiztarget.com] | funksec | Link |
| 2024-12-11 | [Planters Telephone Cooperative (planters.net)] | fog | Link |
| 2024-12-11 | [www.minerasancristobal.com] | apt73 | Link |
| 2024-12-02 | [Westerstrand Urfabrik AB] | bluebox | Link |
| 2024-12-03 | [PH ARCHITECTURE] | bluebox | Link |
| 2024-12-11 | [Matagrano] | akira | Link |
| 2024-12-11 | [Renée Blanche] | akira | Link |
| 2024-12-11 | [Nova Pole International Inc.] | akira | Link |
| 2024-12-11 | [Rutherford County Schools] | rhysida | Link |
| 2024-12-11 | [mandiricoal.net] | funksec | Link |
| 2024-12-11 | [dealplexus.com] | funksec | Link |
| 2024-12-10 | [Inmobiliaria Armas] | medusa | Link |
| 2024-12-10 | [Bergerhof] | medusa | Link |
| 2024-12-10 | [Ainsworth Game Technology Limited] | medusa | Link |
| 2024-12-10 | [Hydra-Matic Packing] | lynx | Link |
| 2024-12-10 | [singularanalysts.com] | funksec | Link |
| 2024-12-10 | [gervetusa.com] | funksec | Link |
| 2024-12-10 | [fpsc-anz.com] | funksec | Link |
| 2024-12-10 | [Orthopaedie-hof.de] | cloak | Link |
| 2024-12-10 | [Ukh-hof.de] | cloak | Link |
| 2024-12-10 | [www.appicgarage.com] | funksec | Link |
| 2024-12-10 | [wacer.com.au] | funksec | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-10 | [thebetareview.com] | funksec | Link |
| 2024-12-10 | [senseis.xmp.net] | funksec | Link |
| 2024-12-10 | [fpsc-anz.com Breach] | funksec | Link |
| 2024-12-10 | [tectaamerica.com] | ransomhub | Link |
| 2024-12-10 | [Mission Constructors , Inc.] | nitrogen | Link |
| 2024-12-10 | [Haji Husein Alireza] | incransom | Link |
| 2024-12-10 | [kurosu.com.py] | funksec | Link |
| 2024-12-10 | [workers.com.zm] | funksec | Link |
| 2024-12-10 | [leadboxhq.com] | apt73 | Link |
| 2024-12-10 | [Matandy (matandy.com)] | akira | Link |
| 2024-12-10 | [workers.com.zm Breach] | funksec | Link |
| 2024-12-10 | [Corporación BJR] | akira | Link |
| 2024-12-10 | [Global Insurance Agency LLC] | bianlian | Link |
| 2024-12-10 | [Conrey Insurance Brokers & Risk Managers] | akira | Link |
| 2024-12-10 | [Aruba Productions] | akira | Link |
| 2024-12-10 | [Lakeside Sod Supply] | akira | Link |
| 2024-12-09 | [Proyectos y Seguros] | akira | Link |
| 2024-12-10 | [womenscare.com] | ransomhub | Link |
| 2024-12-10 | [greenscape.us.com] | ransomhub | Link |
| 2024-12-10 | [Physicians' Primary Care of Southwest Florida] | bianlian | Link |
| 2024-12-10 | [nedamaritime.gr] | blackout | Link |
| 2024-12-03 | [Equity & Advisory] | lynx | Link |
| 2024-12-10 | [kurosu.com.py Breach] | funksec | Link |
| 2024-12-09 | [gervetusa.com Breach] | funksec | Link |
| 2024-12-09 | [singularanalysts.com Breach] | funksec | Link |
| 2024-12-04 | [www.lasalleinc.com] | ransomhub | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-09 | [inia.es] | ransomhub | Link |
| 2024-12-09 | [precisediagnosticspacs warn] | funksec | Link |
| 2024-12-09 | [melhorcompraclube.com.br] | apt73 | Link |
| 2024-12-09 | [Hosting.co.uk] | lynx | Link |
| 2024-12-09 | [sincorpe.org.br] | funksec | Link |
| 2024-12-09 | [pti.agency] | funksec | Link |
| 2024-12-09 | [www.bms.com] | apt73 | Link |
| 2024-12-09 | [bankily.mr] | apt73 | Link |
| 2024-12-09 | [Cipla] | akira | Link |
| 2024-12-09 | [Consumers Builders Supply] | akira | Link |
| 2024-12-09 | [ECBM] | akira | Link |
| 2024-12-06 | [Pelstar] | akira | Link |
| 2024-12-06 | [Pb Loader] | akira | Link |
| 2024-12-06 | [Jamaica Bearings Group] | akira | Link |
| 2024-12-06 | [Weinberg & Schwartz LLC] | akira | Link |
| 2024-12-05 | [Milwaukee Cylinder] | akira | Link |
| 2024-12-05 | [Davis Immigration Law Office] | akira | Link |
| 2024-12-05 | [Séguin Haché SENCRL] | akira | Link |
| 2024-12-04 | [Coffee Beanery] | akira | Link |
| 2024-12-04 | [C Pathe] | akira | Link |
| 2024-12-09 | [Boston Chinatown Neighborhood Center] | interlock | Link |
| 2024-12-08 | [spdyn.de technology] | funksec | Link |
| 2024-12-08 | [ncfe.org.in] | funksec | Link |
| 2024-12-08 | [Gulf Petrochemical Services & Trading] | sarcoma | Link |
| 2024-12-07 | [uniamarmores] | funksec | Link |
| 2024-12-07 | [zero5] | funksec | Link |
| 2024-12-07 | [FunkLocker] | funksec | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-07 | [Matlock Security Services] | rhysida | Link |
| 2024-12-07 | [ayswrewards] | funksec | Link |
| 2024-12-07 | [Arc Community Services Inc] | incransom | Link |
| 2024-12-07 | [CO-VER Power Technology SpA] | everest | Link |
| 2024-12-06 | [T&M Equipment] | kairos | Link |
| 2024-12-06 | [RJM Marketing] | interlock | Link |
| 2024-12-06 | [Medical Technology Industries, Inc.] | everest | Link |
| 2024-12-05 | [Brodsky Renehan Pearlstein & Bouquet, Chartered] | medusa | Link |
| 2024-12-06 | [Precision Walls] | dragonforce | Link |
| 2024-12-05 | [Levicoff Law Firm, P.C] | medusa | Link |
| 2024-12-06 | [mtgazeta.uz] | funksec | Link |
| 2024-12-06 | [LTI Trucking Services] | bianlian | Link |
| 2024-12-06 | [Blue Yonder] | termite | Link |
| 2024-12-06 | [pro-mec.com] | ransomhub | Link |
| 2024-12-06 | [Pan Gulf Holding] | sarcoma | Link |
| 2024-12-06 | [pez.com] | abyss | Link |
| 2024-12-05 | [ctsjo.com] | funksec | Link |
| 2024-12-05 | [Standard Calibrations] | play | Link |
| 2024-12-05 | [NatAlliance Securities] | play | Link |
| 2024-12-05 | [ITO EN] | play | Link |
| 2024-12-05 | [Max Trans] | play | Link |
| 2024-12-05 | [azpay.me] | apt73 | Link |
| 2024-12-05 | [SRP Federal Credit Union] | nitrogen | Link |
| 2024-12-05 | [Anonymous Victim] | sarcoma | Link |
| 2024-12-05 | [Dorner (dorner-gmbh.de)] | fog | Link |
| 2024-12-05 | [Star Shuttle Inc.] | bianlian | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-05 | [hanwhacimarron.com] | ransomhub | Link |
| 2024-12-05 | [edizionidottrinari] | funksec | Link |
| 2024-12-05 | [altuslab] | funksec | Link |
| 2024-12-04 | [frigopesca.com.ec] | ransomhub | Link |
| 2024-12-05 | [USA2ME] | killsec | Link |
| 2024-12-05 | [www.aliorbank.pl] | apt73 | Link |
| 2024-12-04 | [Donnewalddistributing] | cloak | Link |
| 2024-12-04 | [islandphoto.com] | ransomhub | Link |
| 2024-12-04 | [troxlerlabs.com] | ransomhub | Link |
| 2024-12-04 | [hobokennj.gov] | threeam | Link |
| 2024-12-04 | [NTrust] | raworld | Link |
| 2024-12-04 | [copral.com.br] | lockbit3 | Link |
| 2024-12-04 | [Deloitte UK] | BrainCipher | Link |
| 2024-12-04 | [uniaomarmores] | funksec | Link |
| 2024-12-04 | [westbankcorp.com] | blackbasta | Link |
| 2024-12-04 | [snatt.it] | blackbasta | Link |
| 2024-12-04 | [vossko.de] | blackbasta | Link |
| 2024-12-04 | [www.certifiedinfosec.com] | apt73 | Link |
| 2024-12-04 | [FF Steel] | sarcoma | Link |
| 2024-12-03 | [www.sefiso-atlantique.fr] | ransomhub | Link |
| 2024-12-03 | [marietta-city.org] | ransomhub | Link |
| 2024-12-03 | [westbornmarket.com] | ransomhub | Link |
| 2024-12-04 | [www.lasalle.com] | ransomhub | Link |
| 2024-12-04 | [kingdom] | funksec | Link |
| 2024-12-04 | [albazaar] | funksec | Link |
| 2024-12-04 | [rscn.org.jo] | funksec | Link |
| 2024-12-04 | [verificativa] | funksec | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-04 | [intbizth] | funksec | Link |
| 2024-12-04 | [xui.one] | funksec | Link |
| 2024-12-04 | [x-cart automotive] | funksec | Link |
| 2024-12-04 | [IFA Paris] | funksec | Link |
| 2024-12-04 | [styched] | funksec | Link |
| 2024-12-04 | [Smart-it-partner] | funksec | Link |
| 2024-12-04 | [USA Network] | funksec | Link |
| 2024-12-04 | [Zero 5] | funksec | Link |
| 2024-12-03 | [Marine Stores Guide] | qilin | Link |
| 2024-12-03 | [www.giorgiovisconti.it] | ransomhub | Link |
| 2024-12-03 | [www.goethe-university-frankfurt.de] | ransomhub | Link |
| 2024-12-03 | [www.siapenet.gov.br] | apt73 | Link |
| 2024-12-03 | [InterCon Construction] | hunters | Link |
| 2024-12-03 | [Conteg] | hunters | Link |
| 2024-12-03 | [Royce Corporation] | BrainCipher | Link |
| 2024-12-03 | [ACM_IT] | argonauts | Link |
| 2024-12-03 | [RDC] | argonauts | Link |
| 2024-12-03 | [Goodwill North Central Texas] | rhysida | Link |
| 2024-12-03 | [Harel Insurance ( Shirbit Server )] | handala | Link |
| 2024-12-02 | [New Age Micro] | lynx | Link |
| 2024-12-02 | [Billaud Segeba] | qilin | Link |
| 2024-12-02 | [salesgig.com] | darkvault | Link |
| 2024-12-02 | [KHKKLOW.com] | ransomhub | Link |
| 2024-12-02 | [G-ONE AUTO PARTS DE MÉXICO, S.A. DE C.V.] | BrainCipher | Link |
| 2024-12-02 | [Conlin’s Pharmacy (conlinspharmacy.com)] | fog | Link |
| 2024-12-02 | [Mmaynewagemicro] | lynx | Link |
| 2024-12-02 | [Avico Spice] | medusa | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-12-02 | [Down East Granite] | medusa | Link |
| 2024-12-02 | [Wiley Metal Fabricating] | medusa | Link |
| 2024-12-01 | [shapesmfg.com] | ransomhub | Link |
| 2024-12-01 | [qualitybillingservice.com] | ransomhub | Link |
| 2024-12-01 | [tascosaofficemachines.com] | ransomhub | Link |
| 2024-12-01 | [costelloeye.com] | ransomhub | Link |
| 2024-12-01 | [McKibbin] | incransom | Link |
| 2024-12-01 | [Alpine Ear Nose & Throat] | bianlian | Link |

# 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
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

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.