
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20241121



Inhaltsverzeichnis

| | |
|---|-----------|
| 1 Editorial | 2 |
| 2 Security-News | 3 |
| 2.1 Heise - Security-Alert | 3 |
| 3 Sicherheitslücken | 4 |
| 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 |
| 4 Aktiv ausgenutzte Sicherheitslücken | 13 |
| 4.1 Exploits der letzten 5 Tage | 13 |
| 4.2 0-Days der letzten 5 Tage | 17 |
| 5 Die Hacks der Woche | 21 |
| 5.0.1 Sophos spielt die UNO Reverse Karte ☒ (+ Redline Stealer) | 21 |
| 6 Cyberangriffe: (Nov) | 22 |
| 7 Ransomware-Erpressungen: (Nov) | 22 |
| 8 Quellen | 37 |
| 8.1 Quellenverzeichnis | 37 |
| 9 Impressum | 38 |

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

Trend Micros Deep Security Agent ermöglicht Einschleusen von Schadcode

Angreifer können Trend Micros Deep Security Agent Schadcode unterjubeln, etwa auch im lokalen Netz. Admins sollten zügig aktualisieren.

- [Link](#)

—

Angreifer attackieren Oracle Agile PLM

Oracle hat aufgrund von laufenden Attacken auf Oracle Agile Product Lifecycle Management ein Sicherheitsupdate außer der Reihe veröffentlicht.

- [Link](#)

—

Apache OfBiz: Schwachstelle ermöglicht Codeschmuggel

Eine aktualisierte Version der ERP-Software Apache OfBiz schließt Sicherheitslecks, die das Ausführen von Schadcode ermöglichen.

- [Link](#)

—

Sicherheitslücke: Azure Stack HCI für Attacke anfällig

Microsoft hat einen wichtigen Sicherheitspatch für Azure Stack HCI veröffentlicht. Bislang wurden noch keine Attacken beobachtet.

- [Link](#)

—

Sicherheitsupdates für Nextcloud: Unberechtigte Zugriffe möglich

Mehrere Komponenten von Nextcloud sind verwundbar. Admins sollten ihre Instanzen zeitnah mittels verfügbarer Sicherheitspatches absichern.

- [Link](#)

—

Lücken in FortiClient, Kemp Loadmaster, PAN-OS und VMware vCenter attackiert

Kriminelle attackieren aktuell teils ungepatchte Sicherheitslücken in FortiClient, Kemp Loadmaster, PAN-OS und VMware vCenter.

- [Link](#)

—

Kritische Palo-Alto-Lücke: Details und Patches sind da, CISA warnt vor Exploit

Fast drei Wochen nach ersten Exploit-Gerüchten hat der Hersteller nun endlich reagiert, trickst aber. Derweil warnt die US-Cyberbehörde vor Angriffen.

- [Link](#)

Sicherheitsupdates: PostgreSQL für Schadcode-Attacken anfällig

Das Datenbankmanagementsystem PostgreSQL ist über mehrere Lücken angreifbar. Admins sollten Instanzen jetzt absichern. Für eine Version läuft der Support aus.

- [Link](#)

Palo-Alto: Ungepatchter Zero-Day für Security-Appliances wird ausgenutzt

In der vergangenen Woche hatte Palo Alto Kunden über eine ungepatchte Lücke im Webinterface verschiedener Firewalls informiert. Diese wird nun ausgenutzt.

- [Link](#)

Wordpress-Plug-in Really Simple Security gefährdet 4 Millionen Websites

Rund vier Millionen Wordpress-Seiten nutzen das Plug-in Really Simple Security. Angreifer aus dem Netz können sie kompromittieren.

- [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 | 0.955020000 | 0.994610000 | Link |
| CVE-2023-6895 | 0.936280000 | 0.992140000 | Link |
| CVE-2023-6553 | 0.951250000 | 0.994000000 | Link |
| CVE-2023-6019 | 0.932040000 | 0.991660000 | Link |
| CVE-2023-6018 | 0.911590000 | 0.989990000 | Link |
| CVE-2023-52251 | 0.947690000 | 0.993520000 | Link |
| CVE-2023-4966 | 0.970550000 | 0.998150000 | Link |
| CVE-2023-49103 | 0.951130000 | 0.993980000 | Link |
| CVE-2023-48795 | 0.962880000 | 0.995940000 | Link |
| CVE-2023-47246 | 0.962620000 | 0.995870000 | Link |
| CVE-2023-46805 | 0.959100000 | 0.995290000 | Link |
| CVE-2023-46747 | 0.972560000 | 0.998850000 | Link |
| CVE-2023-46604 | 0.969640000 | 0.997790000 | Link |
| CVE-2023-4542 | 0.941060000 | 0.992670000 | Link |
| CVE-2023-43208 | 0.974790000 | 0.999770000 | Link |
| CVE-2023-43177 | 0.961030000 | 0.995600000 | Link |
| CVE-2023-42793 | 0.970830000 | 0.998240000 | Link |
| CVE-2023-41892 | 0.905460000 | 0.989510000 | Link |
| CVE-2023-41265 | 0.912600000 | 0.990040000 | Link |
| CVE-2023-38205 | 0.958720000 | 0.995220000 | Link |
| CVE-2023-38203 | 0.964750000 | 0.996380000 | Link |
| CVE-2023-38146 | 0.920950000 | 0.990630000 | Link |
| CVE-2023-38035 | 0.974360000 | 0.999600000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-36845 | 0.968430000 | 0.997460000 | Link |
| CVE-2023-3519 | 0.965540000 | 0.996620000 | Link |
| CVE-2023-35082 | 0.963840000 | 0.996190000 | Link |
| CVE-2023-35078 | 0.967840000 | 0.997300000 | Link |
| CVE-2023-34993 | 0.973050000 | 0.999030000 | Link |
| CVE-2023-34634 | 0.926130000 | 0.991050000 | Link |
| CVE-2023-34362 | 0.969380000 | 0.997710000 | Link |
| CVE-2023-34039 | 0.929610000 | 0.991440000 | Link |
| CVE-2023-3368 | 0.930810000 | 0.991560000 | Link |
| CVE-2023-33246 | 0.973040000 | 0.999030000 | Link |
| CVE-2023-32315 | 0.973370000 | 0.999160000 | Link |
| CVE-2023-32235 | 0.910390000 | 0.989880000 | Link |
| CVE-2023-30625 | 0.954240000 | 0.994490000 | Link |
| CVE-2023-30013 | 0.966660000 | 0.996930000 | Link |
| CVE-2023-29300 | 0.967820000 | 0.997290000 | Link |
| CVE-2023-29298 | 0.968380000 | 0.997450000 | Link |
| CVE-2023-28432 | 0.906870000 | 0.989630000 | Link |
| CVE-2023-28343 | 0.966250000 | 0.996790000 | Link |
| CVE-2023-28121 | 0.929810000 | 0.991460000 | Link |
| CVE-2023-27524 | 0.970320000 | 0.998050000 | Link |
| CVE-2023-27372 | 0.973870000 | 0.999390000 | Link |
| CVE-2023-27350 | 0.969220000 | 0.997660000 | Link |
| CVE-2023-26469 | 0.958860000 | 0.995250000 | Link |
| CVE-2023-26360 | 0.962010000 | 0.995780000 | Link |
| CVE-2023-26035 | 0.969120000 | 0.997630000 | Link |
| CVE-2023-25717 | 0.949440000 | 0.993730000 | Link |
| CVE-2023-25194 | 0.967670000 | 0.997260000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-2479 | 0.961940000 | 0.995770000 | Link |
| CVE-2023-24489 | 0.972890000 | 0.998970000 | Link |
| CVE-2023-23752 | 0.948310000 | 0.993610000 | Link |
| CVE-2023-23397 | 0.902750000 | 0.989360000 | Link |
| CVE-2023-23333 | 0.963300000 | 0.996060000 | Link |
| CVE-2023-22527 | 0.970570000 | 0.998150000 | Link |
| CVE-2023-22518 | 0.963120000 | 0.996020000 | Link |
| CVE-2023-22515 | 0.973360000 | 0.999150000 | Link |
| CVE-2023-21839 | 0.933960000 | 0.991880000 | Link |
| CVE-2023-21554 | 0.951950000 | 0.994110000 | Link |
| CVE-2023-20887 | 0.968860000 | 0.997550000 | Link |
| CVE-2023-1698 | 0.916400000 | 0.990270000 | Link |
| CVE-2023-1671 | 0.962610000 | 0.995870000 | Link |
| CVE-2023-0669 | 0.971930000 | 0.998600000 | Link |

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 20 Nov 2024

[NEU] [hoch] M-Files Server: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in M-Files Server ausnutzen, um Informationen offenzulegen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Wed, 20 Nov 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—
Wed, 20 Nov 2024

[UPDATE] [hoch] GNU Emacs: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GNU Emacs ausnutzen, um beliebigen Programmcode auszuführen oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—
Wed, 20 Nov 2024

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

Ein Angreifer kann mehrere Schwachstellen in Red Hat Satellite ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren, HTTP-Request-Smuggling-Angriffe durchzuführen oder Phishing- und Cross-Site-Scripting (XSS)-Angriffe auszuführen.

- [Link](#)

—
Wed, 20 Nov 2024

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

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

- [Link](#)

—
Wed, 20 Nov 2024

[UPDATE] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—
Wed, 20 Nov 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR und Thunderbird: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Mozilla Firefox, Firefox ESR und Thunderbird ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—
Wed, 20 Nov 2024

[UPDATE] [hoch] Apache Camel und mehrere Red Hat Produkte: Mehrere Schwachstellen

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Apache Camel und in mehreren Red Hat-Produkten ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben und beliebigen Code auszuführen.

- [Link](#)

—

Wed, 20 Nov 2024

[UPDATE] [kritisch] Red Hat Enterprise Linux: Mehrere Schwachstellen

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

- [Link](#)

—

Wed, 20 Nov 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](#)

—

Wed, 20 Nov 2024

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

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

- [Link](#)

—

Wed, 20 Nov 2024

[UPDATE] [hoch] X.Org X11 und Xming: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in X.Org X11 und Xming ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 20 Nov 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (OpenEXR): Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Wed, 20 Nov 2024

[UPDATE] [hoch] Red Hat OpenShift: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat OpenShift ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- [Link](#)

—

Wed, 20 Nov 2024

[UPDATE] [hoch] Microsoft DeveloperTools: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio Code, Microsoft Visual Studio 2022 und Microsoft Windows ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Wed, 20 Nov 2024

[UPDATE] [hoch] Apache Camel for Spring Boot: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Apache Camel for Spring Boot ausnutzen, um beliebigen Code auszuführen oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 20 Nov 2024

[NEU] [hoch] Apple Safari, iOS, iPadOS, macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple Safari, Apple iOS, Apple iPadOS und Apple macOS ausnutzen, um beliebigen Programmcode auszuführen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Wed, 20 Nov 2024

[NEU] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 19 Nov 2024

[UPDATE] [hoch] Apple iOS und iPadOS: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apple iOS und Apple iPadOS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 19 Nov 2024

[UPDATE] [hoch] Ubiquiti UniFi: Schwachstelle ermöglicht Privilegieneskalation

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

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|------------|--|-----------|
| 11/20/2024 | [Oracle Linux 9 : krb5 (ELSA-2024-9474)] | critical |
| 11/20/2024 | [Oracle Linux 9 : grafana (ELSA-2024-9473)] | critical |
| 11/19/2024 | [GeoVision GV-ADR2701 Improper Authentication (CVE-2023-3638)] | critical |
| 11/20/2024 | [Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel (Low Latency) vulnerabilities (USN-7089-7)] | high |
| 11/20/2024 | [Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7121-1)] | high |
| 11/20/2024 | [Ubuntu 20.04 LTS : Linux kernel (IoT) vulnerabilities (USN-7119-1)] | high |
| 11/20/2024 | [Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel vulnerabilities (USN-7120-1)] | high |
| 11/20/2024 | [Ubuntu 14.04 LTS : Linux kernel vulnerability (USN-7122-1)] | high |
| 11/20/2024 | [Photon OS 3.0: Linux PHSA-2024-3.0-0804] | high |
| 11/20/2024 | [Palo Alto Networks PAN-OS 10.2.x < 10.2.11 / 11.0.x < 11.0.6 / 11.1.x < 11.1.5 Vulnerability] | high |
| 11/20/2024 | [ManageEngine ADAudit Plus < Build 8123 SQLi (CVE-2024-49574)] | high |

| Datum | Schwachstelle | Bewertung |
|------------|--|-----------|
| 11/20/2024 | [Draytek VigorConnect Unauthenticated LFI (CVE-2021-20124)] | high |
| 11/20/2024 | [Palo Alto Networks PAN-OS 10.2.x < 10.2.7-h16 / 11.1.x < 11.1.2-h14 / 11.2.x < 11.2.2-h3 Vulnerability] | high |
| 11/20/2024 | [aioHTTP 3.10.6 < 3.10.11 Memory Leak] | high |
| 11/20/2024 | [Fedora 39 : chromium (2024-9c44ad3527)] | high |
| 11/20/2024 | [Fedora 41 : llvm-test-suite (2024-6d9aba8c3c)] | high |
| 11/20/2024 | [Fedora 40 : llvm-test-suite (2024-300397332b)] | high |
| 11/20/2024 | [AlmaLinux 9 : kernel (ALSA-2024:9605)] | high |
| 11/20/2024 | [Ubuntu 14.04 LTS : Linux kernel (Azure) vulnerabilities (USN-7121-2)] | high |
| 11/20/2024 | [Ubuntu 22.04 LTS / 24.04 LTS : Linux kernel vulnerabilities (USN-7120-2)] | high |
| 11/20/2024 | [Ubuntu 22.04 LTS : Linux kernel (Azure) vulnerabilities (USN-7123-1)] | high |
| 11/20/2024 | [PostgreSQL 12.x < 12.21 / 13.x < 13.17 / 14.x < 14.14 / 15.x < 15.9 / 16.x < 16.5 / 17.x < 17.1 Multiple Vulnerabilities] | high |
| 11/20/2024 | [Drupal 7.x < 7.102 / 10.2.x < 10.2.11 / 10.3.x < 10.3.9 / 11.x < 11.0.8 Multiple Vulnerabilities (drupal-2024-11-20)] | high |
| 11/20/2024 | [Wireshark 4.2.x < 4.2.9 Multiple Vulnerabilities] | high |
| 11/20/2024 | [Wireshark 4.2.x < 4.2.9 Multiple Vulnerabilities (macOS)] | high |
| 11/20/2024 | [Oracle Linux 9 : tigervnc (ELSA-2024-10090)] | high |
| 11/20/2024 | [Oracle Linux 9 : python3.9 (ELSA-2024-9468)] | high |
| 11/20/2024 | [Oracle Linux 9 : grafana-pcp (ELSA-2024-9472)] | high |
| 11/19/2024 | [Schneider PowerLogic PM5300 Series Uncontrolled Resource Consumption (CVE-2024-9409)] | high |

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Tue, 19 Nov 2024

WordPress Really Simple Security Authentication Bypass

WordPress Really Simple Security plugin versions prior to 9.1.2 proof of concept authentication bypass exploit.

- [Link](#)

—

” “Tue, 19 Nov 2024

Palo Alto PAN-OS Authentication Bypass / Remote Command Execution

Proof of concept code to exploit an authentication bypass in Palo Alto's PAN-OS that is coupled with remote command execution.

- [Link](#)

—

” “Mon, 18 Nov 2024

Pyload Remote Code Execution

CVE-2024-28397 is a sandbox escape in js2py versions 0.74 and below. js2py is a popular python package that can evaluate javascript code inside a python interpreter. The vulnerability allows for an attacker to obtain a reference to a python object in the js2py environment enabling them to escape the sandbox, bypass pyimport restrictions and execute arbitrary commands on the host. At the time of this writing no patch has been released and version 0.74 is the latest version of js2py which was released Nov 6, 2022. CVE-2024-39205 is a remote code execution vulnerability in Pyload versions 0.5.0b3.dev85 and below. It is an open-source download manager designed to automate file downloads from various online sources. Pyload is vulnerable because it exposes the vulnerable js2py functionality mentioned above on the /flash/addcrypto2 API endpoint. This endpoint was designed to only accept connections from localhost but by manipulating the HOST header we can bypass this restriction in order to access the API to achieve unauthenticated remote code execution.

- [Link](#)

—

” “Mon, 18 Nov 2024

SOPlanning 1.52.01 Remote Code Execution

SOPlanning version 1.52.01 authenticated remote code execution exploit.

- [Link](#)

—

” “Thu, 14 Nov 2024

Siemens Energy Omnivise T3000 8.2 SP3 Privilege Escalation / File Download

Siemens Energy Omnivise T3000 version 8.2 SP3 suffers from local privilege escalation, cleartext storage of passwords in configuration and log files, file system access allowing for arbitrary file download, and IP whitelist bypass.

- [Link](#)

—

” “Thu, 14 Nov 2024

TX Text Control .NET Server For ASP.NET Arbitrary File Read / Write

TX Text Control .NET Server For ASP.NET has an issue where it was possible to change the configured system path for reading and writing files in the underlying operating system with privileges of the user running a web application.

- [Link](#)

—

” “Thu, 14 Nov 2024

GravCMS 1.10.7 Arbitrary YAML Write / Update

Proof of concept remote code execution exploit for GravCMS 1.10.7 that leverages an arbitrary YAML write / update.

- [Link](#)

—

” “Thu, 14 Nov 2024

PHP-CGI Argument Injection Remote Code Execution

Proof of concept remote code execution exploit for PHP-CGI that affects versions 8.1 before 8.1.29, 8.2 before 8.2.20, and 8.3 before 8.3.8.

- [Link](#)

—

” “Wed, 13 Nov 2024

Palo Alto Expedition 1.2.91 Remote Code Execution

This Metasploit module lets you obtain remote code execution in Palo Alto Expedition versions 1.2.91 and below. The first vulnerability, CVE-2024-5910, allows to reset the password of the admin user, and the second vulnerability, CVE-2024-9464, is an authenticated OS command injection. In a default installation, commands will get executed in the context of www-data. When credentials are provided, this module will only exploit the second vulnerability. If no credentials are provided, the module will first try to reset the admin password and then perform the OS command injection.

- [Link](#)

—

” “Mon, 11 Nov 2024

HASOMED Elephant / Elephant Software Updater Data Exposure / Privilege Escalation

HASOMED Elephant versions prior to 24.04.00 and Elephant Software Updater versions prior to 1.4.2.1811 suffer from having an unprotected exposed firebird database, unprotected FHIR API, multiple local

privilege escalation, and hardcoded service password vulnerabilities.

- [Link](#)

—

” “Mon, 11 Nov 2024

WSO2 4.0.0 / 4.1.0 / 4.2.0 Shell Upload

WSO2 versions 4.0.0, 4.1.0, and 4.2.0 are susceptible to remote code execution via an arbitrary file upload vulnerability.

- [Link](#)

—

” “Thu, 07 Nov 2024

WordPress Meetup 0.1 Authentication Bypass

WordPress Meetup plugin versions 0.1 and below suffer from an authentication bypass vulnerability.

- [Link](#)

—

” “Thu, 07 Nov 2024

CyberPanel upgrademysqlstatus Arbitrary Command Execution

Proof of concept remote command execution exploit for CyberPanel versions prior to 5b08cd6.

- [Link](#)

—

” “Thu, 07 Nov 2024

TestRail CLI FieldsParser eval Injection

While parsing test result XML files with the TestRail CLI, the presence of certain TestRail-specific fields can cause untrusted data to flow into an eval() statement, leading to arbitrary code execution. In order to exploit this, an attacker would need to be able to cause the TestRail CLI to parse a malicious XML file. Normally an attacker with this level of control would already have other avenues of gaining code execution.

- [Link](#)

—

” “Tue, 05 Nov 2024

ABB Cylon Aspect 3.08.00 Off-By-One

A vulnerability was identified in a ABB Cylon Aspect version 3.08.00 where an off-by-one error in array access could lead to undefined behavior and potential denial of service. The issue arises in a loop that iterates over an array using a less than or equals to condition, allowing access to an out-of-bounds index. This can trigger errors or unexpected behavior when processing data, potentially crashing the application. Successful exploitation of this vulnerability can lead to a crash or disruption of service, especially if the script handles large data sets.

- [Link](#)

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 SSH Denial Of Service

Sysax Multi Server version 6.9.9 suffers from an SSH related denial of service vulnerability.

- [Link](#)

—

” “Mon, 04 Nov 2024

Sysax Multi Server 6.99 Cross Site Scripting

Sysax Multi Server version 6.9.9 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 04 Nov 2024

IBM Security Verify Access 32 Vulnerabilities

IBM Security Verify Access versions prior to 10.0.8 suffer from authentication bypass, reuse of private keys, local privilege escalation, weak settings, outdated libraries, missing password, hardcoded secrets, remote code execution, missing authentication, null pointer dereference, and lack of privilege separation vulnerabilities.

- [Link](#)

—

” “Mon, 04 Nov 2024

IBM Security Verify Access Appliance Insecure Transit / Hardcoded Passwords

IBM Security Verify Access Appliance suffers from multiple insecure transit vulnerabilities, hardcoded passwords, and uninitialized variables. ibmsecurity versions prior to 2024.4.5 are affected.

- [Link](#)

—

” “Mon, 04 Nov 2024

ESET NOD32 Antivirus 18.0.12.0 Unquoted Service Path

ESET NOD32 Antivirus version 18.0.12.0 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Mon, 04 Nov 2024

SQLite3 generate_series Stack Buffer Underflow

SQLite3 suffers from a stack buffer underflow condition in seriesBestIndex in the generate_series extension.

- [Link](#)

—

” “Mon, 04 Nov 2024

Linux khugepaged Race Conditions

khugepaged in Linux races with rmap-based zap, races with GUP-fast, and fails to call MMU notifiers.

- [Link](#)

—

” “Fri, 01 Nov 2024

Ping Identity PingIDM 7.5.0 Query Filter Injection

Ping Identity PingIDM versions 7.0.0 through 7.5.0 enabled an attacker with read access to the User collection, to abuse API query filters in order to obtain managed and/or internal user's passwords in either plaintext or encrypted variants, based on configuration. The API clearly prevents the password in either plaintext or encrypted to be retrieved by any other means, as this field is set as protected under the User object. However, by injecting a malicious query filter, using password as the field to be filtered, an attacker can perform a blind brute-force on any victim's user password details (encrypted object or plaintext string).

- [Link](#)

—

” “Fri, 01 Nov 2024

ABB Cylon Aspect 3.08.01 File Upload MD5 Checksum Bypass

ABB Cylon Aspect version 3.08.01 has a vulnerability in caldavInstall.php, caldavInstallAgendav.php, and caldavUpload.php files, where the presence of an EXPERTMODE parameter activates a badassMode feature. This mode allows an unauthenticated attacker to bypass MD5 checksum validation during file uploads. By enabling badassMode and setting the skipChecksum parameter, the system skips integrity verification, allowing attackers to upload or install altered CalDAV zip files without authentication. This vulnerability permits unauthorized file modifications, potentially exposing the system to tampering or malicious uploads.

- [Link](#)

—

” “Fri, 01 Nov 2024

Packet Storm New Exploits For October, 2024

This archive contains all of the 128 exploits added to Packet Storm in October, 2024.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 20 Nov 2024

ZDI-24-1534: Microsoft SharePoint Server FindSpecific Unsafe Reflection Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 20 Nov 2024

ZDI-24-1533: Panda Security Dome PSANHost Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 20 Nov 2024

ZDI-24-1532: 7-Zip Zstandard Decompression Integer Underflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1531: RSA Security SecureID Software Token for Microsoft Windows Uncontrolled Search Path Element Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1530: WordPress Core maybe_unserialize Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1529: Dassault Systèmes eDrawings Viewer X_B File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1528: Dassault Systèmes eDrawings Viewer SAT File Parsing Uninitialized Variable Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1527: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1526: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1525: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1524: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1523: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1522: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1521: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1520: Siemens Tecnomatix Plant Simulation WRL File Parsing Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1519: Siemens Tecnomatix Plant Simulation WRL File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1518: Siemens Tecnomatix Plant Simulation WRL File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1517: McAfee Total Protection Uncontrolled Search Path Element Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1516: Trend Micro Deep Security Agent Manual Scan Command Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1515: (0Day) Hugging Face Transformers Trax Model Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1514: (0Day) Hugging Face Transformers MaskFormer Model Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 19 Nov 2024

ZDI-24-1513: (0Day) Hugging Face Transformers MobileViTV2 Deserialization of Untrusted Data Remote Code Execution Vulnerability

- [Link](#)

—

” “Mon, 18 Nov 2024

ZDI-24-1512: Progress Software WhatsUp Gold getReport Missing Authentication Authentication Bypass Vulnerability

- [Link](#)

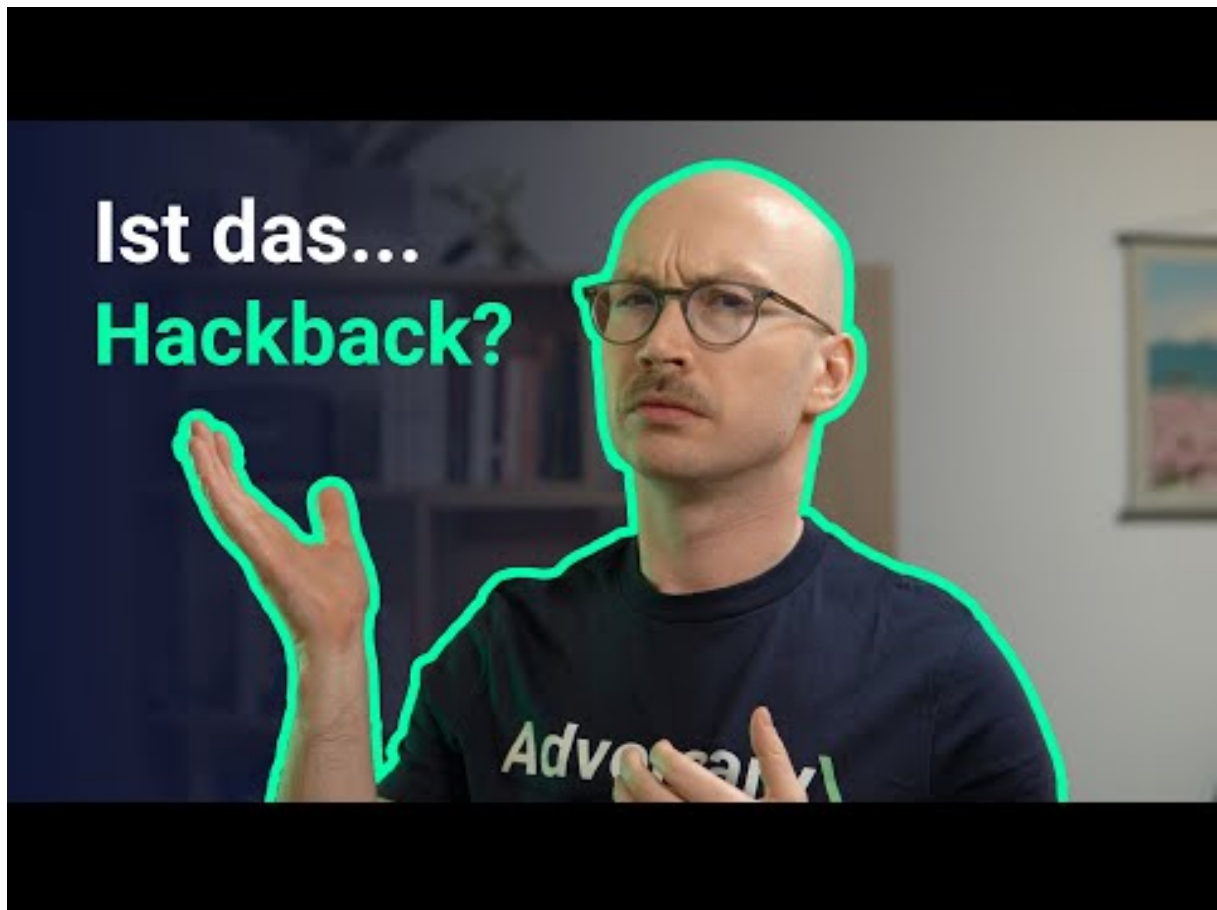
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Sophos spielt die UNO Reverse Karte ☒ (+ Redline Stealer)



[Zum Youtube Video](#)

6 Cyberangriffe: (Nov)

| Datum | Opfer | Land | Information |
|------------|---|-------|----------------------|
| 2024-11-18 | Chambre d'agriculture de la Lozère | [FRA] | Link |
| 2024-11-17 | Bergen auf Rügen | [DEU] | Link |
| 2024-11-13 | Alberta Innovates | [CAN] | Link |
| 2024-11-13 | Cégep de Sorel-Tracy | [CAN] | Link |
| 2024-11-13 | Aschaffenburg | [DEU] | Link |
| 2024-11-13 | Département de la Réunion | [REU] | Link |
| 2024-11-09 | Sheboygan | [USA] | Link |
| 2024-11-09 | Berufsförderungswerk Oberhausen | [DEU] | Link |
| 2024-11-09 | Southern Oregon Veterinary Specialty Center (SOVSC) | [USA] | Link |
| 2024-11-07 | Département des Hautes-Pyrénées | [FRA] | Link |
| 2024-11-07 | Ahold Delhaize | [USA] | Link |
| 2024-11-05 | Lojas Marisa | [BRA] | Link |
| 2024-11-05 | Wexford County | [USA] | Link |
| 2024-11-05 | Ridgewood Schools | [USA] | Link |
| 2024-11-04 | Avis de Torino | [ITA] | Link |
| 2024-11-03 | Washington state courts | [USA] | Link |
| 2024-11-03 | La Sauvegarde | [FRA] | Link |
| 2024-11-03 | Micon Office National | [AUS] | Link |
| 2024-11-02 | Memorial Hospital and Manor | [USA] | Link |
| 2024-11-02 | Kumla kommun | [SWE] | Link |
| 2024-11-01 | South East Technological University (SETU) | [IRL] | Link |

7 Ransomware-Erpressungen: (Nov)

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2024-11-21 | [SSV Blockchain Network] | handala | Link |
| 2024-11-20 | [PK Mulyo] | arcusmedia | Link |
| 2024-11-20 | [Barneek Safety Consultancies] | arcusmedia | Link |
| 2024-11-20 | [Trust Seeds] | arcusmedia | Link |
| 2024-11-20 | [HM Environmental Services] | arcusmedia | Link |
| 2024-11-20 | [IT Networks] | arcusmedia | Link |
| 2024-11-20 | [www.microlise.com] | safepay | Link |
| 2024-11-04 | [Groupe PPA- Mahe] | qilin | Link |
| 2024-11-07 | [Berman Law Group] | qilin | Link |
| 2024-11-07 | [Berman Law Group] | qilin | Link |
| 2024-11-07 | [Prime Group US] | qilin | Link |
| 2024-11-07 | [Prime Group US] | qilin | Link |
| 2024-11-11 | [www.ekirkpatrick.com] | qilin | Link |
| 2024-11-14 | [LaMear & Rapert, LLC - Accounting Firm] | qilin | Link |
| 2024-11-19 | [Alpha Care Medical Group] | qilin | Link |
| 2024-11-19 | [Alpha Care Medical Group] | qilin | Link |
| 2024-11-20 | [Privat Spitex] | qilin | Link |
| 2024-11-20 | [James H Maloy] | akira | Link |
| 2024-11-20 | [Automation Tool & Die] | akira | Link |
| 2024-11-20 | [Tampa State Bank] | akira | Link |
| 2024-11-20 | [Ship Services] | akira | Link |
| 2024-11-19 | [Volo Internet Tech] | akira | Link |
| 2024-11-19 | [Furniture Mart USA] | akira | Link |
| 2024-11-04 | [PBS AEROSPACE] | incransom | Link |
| 2024-11-20 | [RDS Electric] | medusa | Link |
| 2024-11-20 | [Bishop Ireton High School] | rhysida | Link |
| 2024-11-20 | [scalar.co.il] | ransomhub | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------------|-------------------|----------------------|
| 2024-11-20 | [CK Power Public Manufacturing] | hunters | Link |
| 2024-11-20 | [inthinking.net] | darkvault | Link |
| 2024-11-20 | [Amherstburg Family Health] | bianlian | Link |
| 2024-11-19 | [polaraire.com] | ransomhub | Link |
| 2024-11-14 | [Département de La Réunion] | termite | Link |
| 2024-11-20 | [Oxford Auto Insurance] | monti | Link |
| 2024-11-20 | [Camim] | killsec | Link |
| 2024-11-20 | [LiquiTech] | killsec | Link |
| 2024-11-19 | [piburners.com] | safepay | Link |
| 2024-11-19 | [triton sourcing.co.nz] | safepay | Link |
| 2024-11-19 | [onnicar.it] | safepay | Link |
| 2024-11-19 | [kingswoodpark.ca] | safepay | Link |
| 2024-11-19 | [incocommercial.com] | safepay | Link |
| 2024-11-19 | [euromedix.com] | safepay | Link |
| 2024-11-19 | [BusinessTraining.be] | safepay | Link |
| 2024-11-19 | [ccseniorservices] | safepay | Link |
| 2024-11-19 | [ib-spieth.de] | safepay | Link |
| 2024-11-19 | [Safex.us] | safepay | Link |
| 2024-11-19 | [millerservicecompany.com] | safepay | Link |
| 2024-11-19 | [mcauslan.com] | safepay | Link |
| 2024-11-19 | [stats.gov.bb] | safepay | Link |
| 2024-11-19 | [smartdimensions] | safepay | Link |
| 2024-11-19 | [westwood] | safepay | Link |
| 2024-11-19 | [threadfxinc/bluedogmerch] | safepay | Link |
| 2024-11-19 | [Indesign, LLC] | interlock | Link |
| 2024-11-19 | [Henderson Stamping & Production] | play | Link |
| 2024-11-19 | [Diamond Brand Gear] | play | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2024-11-19 | [Dairy Farmers of Canada] | play | Link |
| 2024-11-19 | [Miller & Smith] | play | Link |
| 2024-11-19 | [Hive Power Engineering] | play | Link |
| 2024-11-19 | [CMD] | play | Link |
| 2024-11-19 | [IVC Technologies] | play | Link |
| 2024-11-19 | [Birdair] | play | Link |
| 2024-11-19 | [Vox Printing] | play | Link |
| 2024-11-19 | [Burkburnett Independent School District] | fog | Link |
| 2024-11-19 | [Valley Planing Mill (valleyplaning.com)] | fog | Link |
| 2024-11-19 | [IndicaOnline] | everest | Link |
| 2024-11-19 | [arabot.io] | darkvault | Link |
| 2024-11-19 | [Performance Health & Fitness] | hunters | Link |
| 2024-11-19 | [techguard.in] | darkvault | Link |
| 2024-11-18 | [wulffco.com] | ransomhub | Link |
| 2024-11-19 | [smawins.net] | ransomhub | Link |
| 2024-11-19 | [chsplumbing.com] | ransomhub | Link |
| 2024-11-19 | [tempaircompany.com] | ransomhub | Link |
| 2024-11-19 | [Anderson Miller LTD] | monti | Link |
| 2024-11-19 | [Premier Tax Services] | monti | Link |
| 2024-11-19 | [KVF] | monti | Link |
| 2024-11-19 | [Southern Oregon Veterinary Specialty Center] | monti | Link |
| 2024-11-19 | [rembe.de] | blackbasta | Link |
| 2024-11-19 | [brylesresearch.com] | ransomhub | Link |
| 2024-11-19 | [hartmannbund.de] | ransomhub | Link |
| 2024-11-19 | [citywestcommercials.co.uk] | ransomhub | Link |
| 2024-11-07 | [thinkecs.com] | ransomhub | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2024-11-19 | [San Francisco Ballet] | meow | Link |
| 2024-11-19 | [gfemlaw.com] | blackbasta | Link |
| 2024-11-19 | [instinctpetfood.com] | blackbasta | Link |
| 2024-11-19 | [eatonmetal.com] | blackbasta | Link |
| 2024-11-19 | [continentalserves.com] | blackbasta | Link |
| 2024-11-19 | [wachter.com] | blackbasta | Link |
| 2024-11-19 | [jonti-craft.com] | blackbasta | Link |
| 2024-11-19 | [isaitaly.com] | blackbasta | Link |
| 2024-11-19 | [rockportmortgage.com] | blackbasta | Link |
| 2024-11-19 | [kmcglobal.com] | blackbasta | Link |
| 2024-11-19 | [rauch.de] | blackbasta | Link |
| 2024-11-19 | [interborosd.org] | ransomhub | Link |
| 2024-11-19 | [Thebike.com] | ransomhub | Link |
| 2024-11-19 | [3ccaresystems.com] | ransomhub | Link |
| 2024-11-19 | [Equentis Wealth] | killsec | Link |
| 2024-11-19 | [Terra Energy] | killsec | Link |
| 2024-11-19 | [Find Great People1] | akira | Link |
| 2024-11-06 | [www.depewgillen.com] | ransomhub | Link |
| 2024-11-18 | [Fleet Equipment Center, Inc.] | ElDorado | Link |
| 2024-11-18 | [ATD-American] | ElDorado | Link |
| 2024-11-18 | [K-State College of Veterinary Medicine] | ElDorado | Link |
| 2024-11-18 | [UCC Retrievals, Inc.] | ElDorado | Link |
| 2024-11-18 | [TBM Consulting Group, Inc.] | ElDorado | Link |
| 2024-11-18 | [Premier Packaging] | ElDorado | Link |
| 2024-11-18 | [LINDOSTAR] | ElDorado | Link |
| 2024-11-18 | [Gough Construction] | ElDorado | Link |
| 2024-11-18 | [Programs Improving Public Safety] | ElDorado | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2024-11-18 | [Palm Facility Services] | ElDorado | Link |
| 2024-11-18 | [Kennedy Funding] | ElDorado | Link |
| 2024-11-18 | [BUROTEC S.A.] | ElDorado | Link |
| 2024-11-18 | [A & L Auto Recyclers] | ElDorado | Link |
| 2024-11-18 | [Alliance Industries, LLC.] | ElDorado | Link |
| 2024-11-18 | [CelPlan Technologies, Inc.] | ElDorado | Link |
| 2024-11-18 | [Panzer Solutions LLC Business Services] | ElDorado | Link |
| 2024-11-18 | [The Recycler Core] | ElDorado | Link |
| 2024-11-18 | [Thunderbird Country Club] | ElDorado | Link |
| 2024-11-18 | [Istituto di Istruzione Superiore “Giulio Natta”] | ElDorado | Link |
| 2024-11-18 | [ANKERSKA PLOVIDBA d.d.] | ElDorado | Link |
| 2024-11-18 | [Adams Homes] | ElDorado | Link |
| 2024-11-18 | [A-1 Mobile Lock & Key] | ElDorado | Link |
| 2024-11-18 | [CURVC Corp] | ElDorado | Link |
| 2024-11-18 | [Pensacola] | ElDorado | Link |
| 2024-11-18 | [Think Simple] | ElDorado | Link |
| 2024-11-18 | [Patrick Sanders and Company, P.C.] | ElDorado | Link |
| 2024-11-18 | [Mullen Wylie, LLC] | ElDorado | Link |
| 2024-11-18 | [Cmc Construction Material] | ElDorado | Link |
| 2024-11-18 | [Cucina Tagliani] | ElDorado | Link |
| 2024-11-18 | [Data Campos Sistemas] | ElDorado | Link |
| 2024-11-18 | [GC Custom Metal Fabricationsoon] | ElDorado | Link |
| 2024-11-18 | [Business Systems House FZ-LLC] | ElDorado | Link |
| 2024-11-18 | [Aberdeen] | ElDorado | Link |
| 2024-11-18 | [Compra LTD Aruba] | ElDorado | Link |
| 2024-11-18 | [Minuteman Press] | ElDorado | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2024-11-18 | [Keizer's Collision CSN & Automotive] | ElDorado | Link |
| 2024-11-18 | [The Municipal Administration of Barranquitas and its Department of Finance] | ElDorado | Link |
| 2024-11-18 | [The PHOENIX] | ElDorado | Link |
| 2024-11-18 | [PC AfterHours] | ElDorado | Link |
| 2024-11-18 | [Bells Tax Service] | ElDorado | Link |
| 2024-11-18 | [Tiendas Carrion & Fernandez] | ElDorado | Link |
| 2024-11-01 | [LA LUCKY Brand] | ElDorado | Link |
| 2024-11-18 | [SUSTA S.r.l.] | dragonforce | Link |
| 2024-11-18 | [Maxeon] | medusa | Link |
| 2024-11-18 | [eastgateauto.com] | blacksuit | Link |
| 2024-11-18 | [kciaviation.com] | blacksuit | Link |
| 2024-11-16 | [totaldevelopmentsolutions.com] | ransomhub | Link |
| 2024-11-18 | [jergenspiping.com] | ransomhub | Link |
| 2024-11-18 | [sealevelinc.com] | ransomhub | Link |
| 2024-11-18 | [Jornstax.com] | ransomhub | Link |
| 2024-11-18 | [waive.com.au] | ransomhub | Link |
| 2024-11-18 | [allconstructiongroupwv.com] | ransomhub | Link |
| 2024-11-18 | [Waters Truck and Tractor (waterstruck.com)] | fog | Link |
| 2024-11-18 | [Dorner Law & Title Services] | hunters | Link |
| 2024-11-18 | [Maxus Group] | akira | Link |
| 2024-11-18 | [Bulbrite Industries] | akira | Link |
| 2024-11-18 | [HUTTER ACUSTIX] | akira | Link |
| 2024-11-18 | [Followup CRM] | killsec | Link |
| 2024-11-17 | [Mantinga] | hunters | Link |
| 2024-11-14 | [Apple Electric Ltd] | medusa | Link |
| 2024-11-15 | [LEGO Construction Co] | medusa | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|------------------------------------|-------------------|----------------------|
| 2024-11-15 | [Logistical Software Ltd] | medusa | Link |
| 2024-11-15 | [Manens-Tifs SpA] | medusa | Link |
| 2024-11-14 | [Conseil scolaire Viamonde] | termite | Link |
| 2024-11-13 | [Lebenshilfe Heinsberg] | termite | Link |
| 2024-11-12 | [Oman Oil] | termite | Link |
| 2024-11-12 | [Nifast] | termite | Link |
| 2024-11-16 | [uatf.edu.bo] | stormous | Link |
| 2024-11-15 | [Nunziaplast Srl] | dragonforce | Link |
| 2024-11-15 | [Grupo Trisan] | lynx | Link |
| 2024-11-17 | [Buddy Loan] | killsec | Link |
| 2024-11-17 | [hetrhedens.nl] | blacksuit | Link |
| 2024-11-17 | [texanscan.org] | chort | Link |
| 2024-11-17 | [edwardsburgschoolsfoundation.org] | chort | Link |
| 2024-11-17 | [Tri-TechElectronics.com] | chort | Link |
| 2024-11-17 | [bartow.k12.ga.us] | chort | Link |
| 2024-11-17 | [paaf.gov.kw] | chort | Link |
| 2024-11-17 | [hartwick.edu] | chort | Link |
| 2024-11-17 | [The Egyptian Tax Authority (ETA)] | moneymessage | Link |
| 2024-11-17 | [Dragon Capital] | killsec | Link |
| 2024-11-15 | [kapurinc.com] | blacksuit | Link |
| 2024-11-16 | [American Addiction Centers] | rhysida | Link |
| 2024-11-15 | [Grupo_Trisan] | lynx | Link |
| 2024-11-15 | [klarenbeek-transport.nl] | blacksuit | Link |
| 2024-11-15 | [kenmore.com] | blacksuit | Link |
| 2024-11-15 | [www.gob.mx] | ransomhub | Link |
| 2024-11-15 | [jhs.co.uk] | ransomhub | Link |
| 2024-11-15 | [potteau.com] | ransomhub | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2024-11-15 | [A&O IT Group] | hunters | Link |
| 2024-11-15 | [Vector Transport (vectortransport.com)] | fog | Link |
| 2024-11-15 | [Bio-Clima Service Srl] | everest | Link |
| 2024-11-15 | [Total Patient Care LLC] | everest | Link |
| 2024-11-15 | [A Sensitive Touch Home Health;Alphastar Home Health Care;Heart of Texas Home Healthcare Se] | everest | Link |
| 2024-11-15 | [PHARMATIS-SAS] | incransom | Link |
| 2024-11-13 | [fortinainvestments.com] | ransomhub | Link |
| 2024-11-15 | [BluMed Health] | killsec | Link |
| 2024-11-14 | [Datron WorldCommunications] | akira | Link |
| 2024-11-14 | [Xtrim TVCable] | akira | Link |
| 2024-11-14 | [SKS Bottle &Packaging] | akira | Link |
| 2024-11-14 | [REV Engineering] | akira | Link |
| 2024-11-14 | [Bergeron LLC] | akira | Link |
| 2024-11-14 | [mk Technology Group] | akira | Link |
| 2024-11-14 | [Saint Andrews Bureau] | akira | Link |
| 2024-11-14 | [Ascend Packaging Systems] | akira | Link |
| 2024-11-14 | [Tedkomp AB] | akira | Link |
| 2024-11-14 | [Pemberton Fabricators, Inc (Sexual Harassment videos inside)] | akira | Link |
| 2024-11-14 | [Burmeister &Wain Scandinavian Contractor] | akira | Link |
| 2024-11-14 | [Optical Cable Corporation] | akira | Link |
| 2024-11-14 | [Ultimus] | akira | Link |
| 2024-11-14 | [Tennis Canada] | akira | Link |
| 2024-11-14 | [Don's MobileGlass] | akira | Link |
| 2024-11-14 | [Zyloware] | meow | Link |
| 2024-11-14 | [Pine Belt Cars] | meow | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2024-11-14 | [DieTech North America] | meow | Link |
| 2024-11-14 | [Cottles Asphalt Maintenance Inc] | meow | Link |
| 2024-11-14 | [Herron Todd White] | meow | Link |
| 2024-11-14 | [J.S.T. Espana] | meow | Link |
| 2024-11-14 | [Karl Malone Toyota] | meow | Link |
| 2024-11-14 | [OMara Ag Equipment] | meow | Link |
| 2024-11-14 | [Pincu Barkan, Law Office and Notary] | everest | Link |
| 2024-11-14 | [ADT Freight Services Australia Pty Lt] | sarcoma | Link |
| 2024-11-14 | [Kumla Kommun] | hunters | Link |
| 2024-11-14 | [CP Construplan] | sarcoma | Link |
| 2024-11-13 | [Dumont Printing] | akira | Link |
| 2024-11-13 | [Berexco LLC] | akira | Link |
| 2024-11-13 | [Intercomp] | akira | Link |
| 2024-11-12 | [DynamicSystems] | medusa | Link |
| 2024-11-14 | [Popular Life Insurance] | sarcoma | Link |
| 2024-11-14 | [Micon National] | sarcoma | Link |
| 2024-11-14 | [Kelowna Springs] | sarcoma | Link |
| 2024-11-13 | [stalyhill-inf.tameside.sch.uk] | blacksuit | Link |
| 2024-11-13 | [AXEON 360] | ciphbit | Link |
| 2024-11-13 | [COOPERATIVA TELEFONICA DE CALAFATE LTD.] | BrainCipher | Link |
| 2024-11-13 | [G-One Auto Parts de México S.A. de C.V.] | BrainCipher | Link |
| 2024-11-13 | [Schmack] | hunters | Link |
| 2024-11-13 | [Sercomm] | hunters | Link |
| 2024-11-13 | [midstatesindustrial.com] | threeam | Link |
| 2024-11-13 | [nanolive.ch 2.0] | apt73 | Link |
| 2024-11-05 | [formosacpa.com.tw] | kairos | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2024-11-05 | [askyouraccountant.com] | kairos | Link |
| 2024-11-13 | [kansasrmc.com] | kairos | Link |
| 2024-11-13 | [Value Dental Center] | everest | Link |
| 2024-11-13 | [Artistic Family Dental] | everest | Link |
| 2024-11-13 | [Asaro Dental Aesthetics] | everest | Link |
| 2024-11-13 | [Axpr Valve Science] | killsec | Link |
| 2024-11-12 | [American Associated Pharmacies] | embargo | Link |
| 2024-11-12 | [Giggle Finance] | killsec | Link |
| 2024-11-12 | [Orange County Pathology Medical Group] | raworld | Link |
| 2024-11-12 | [SK Gas] | raworld | Link |
| 2024-11-03 | [Medigroup.ca] | ransomhub | Link |
| 2024-11-12 | [Hillandale Farms] | akira | Link |
| 2024-11-12 | [jst.es] | blacksuit | Link |
| 2024-11-12 | [jarrellimc.com] | blacksuit | Link |
| 2024-11-06 | [Banco de Fomento Internacional] | lynx | Link |
| 2024-11-11 | [TaxPros of Clermont] | lynx | Link |
| 2024-11-11 | [National Institute of Administration] | killsec | Link |
| 2024-11-07 | [DSZ] | lynx | Link |
| 2024-11-07 | [Future Metals] | lynx | Link |
| 2024-11-07 | [Plowman Craven] | lynx | Link |
| 2024-11-11 | [Supply Technologies] | blacksuit | Link |
| 2024-11-11 | [Maxxis International] | blacksuit | Link |
| 2024-11-11 | [potteau.be] | ransomhub | Link |
| 2024-11-11 | [Followmont TransportPty Ltd] | akira | Link |
| 2024-11-11 | [dezinecorp.com] | blacksuit | Link |
| 2024-11-11 | [Amourgis & Associates] | hunters | Link |
| 2024-11-11 | [Dietzgen Corporation] | hunters | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2024-11-01 | [nynewspapers.com] | ransomhub | Link |
| 2024-11-11 | [comarchs.com] | ransomhub | Link |
| 2024-11-11 | [tolbertlegal.com] | ransomhub | Link |
| 2024-11-10 | [OxyHealth] | killsec | Link |
| 2024-11-10 | [Immuno Laboratories, Inc] | bianlian | Link |
| 2024-11-05 | [bitquail.com] | ransomhub | Link |
| 2024-11-09 | [ATSG, Inc] | bianlian | Link |
| 2024-11-09 | [Mizuno (USA)] | bianlian | Link |
| 2024-11-09 | [Palmisano & Goodman, P.A.] | bianlian | Link |
| 2024-11-09 | [Finger Beton Unternehmensgruppe] | meow | Link |
| 2024-11-09 | [Karman Inc] | meow | Link |
| 2024-11-09 | [Siltech (siltechcorp.local)] | lynx | Link |
| 2024-11-09 | [emefarmario.com.br] | apt73 | Link |
| 2024-11-09 | [Granite School District] | rhysida | Link |
| 2024-11-09 | [WimCoCorp] | lynx | Link |
| 2024-11-09 | [NEBRASKALAND] | lynx | Link |
| 2024-11-08 | [MENZIES CNAC (Jardine Aviation Services, Agility)] | spacebears | Link |
| 2024-11-08 | [bartleycorp.com] | ransomhub | Link |
| 2024-11-08 | [interlabel.be] | ransomhub | Link |
| 2024-11-07 | [del-electric.com] | ransomhub | Link |
| 2024-11-08 | [liftkits4less.com] | apt73 | Link |
| 2024-11-08 | [www.lamaisonducitron.com] | apt73 | Link |
| 2024-11-08 | [www.baldinger-ag.ch] | apt73 | Link |
| 2024-11-07 | [Marisa S.A] | medusa | Link |
| 2024-11-08 | [www.assurified.com] | apt73 | Link |
| 2024-11-08 | [www.botiga.com.uy] | apt73 | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2024-11-08 | [Healthcare Management Systems] | bianlian | Link |
| 2024-11-08 | [MedElite Group] | everest | Link |
| 2024-11-07 | [nelconinc.biz] | ransomhub | Link |
| 2024-11-07 | [www.bluco.com] | ransomhub | Link |
| 2024-11-07 | [naj.ae] | darkvault | Link |
| 2024-11-07 | [Equator Worldwide] | meow | Link |
| 2024-11-07 | [Lexco] | meow | Link |
| 2024-11-07 | [europe-qualité] | incransom | Link |
| 2024-11-07 | [Winnebago Public School Foundation] | interlock | Link |
| 2024-11-05 | [Alliance Technical Group] | medusa | Link |
| 2024-11-06 | [Jomar Electrical Contractors] | medusa | Link |
| 2024-11-06 | [Howell Electric Inc] | medusa | Link |
| 2024-11-06 | [www.msdl.ca] | ransomhub | Link |
| 2024-11-07 | [Postcard Mania] | play | Link |
| 2024-11-07 | [New Law] | hunters | Link |
| 2024-11-06 | [klinkamkurpark] | helldown | Link |
| 2024-11-06 | [AMERICANVENTURE] | helldown | Link |
| 2024-11-06 | [CSIKBS] | helldown | Link |
| 2024-11-06 | [SANJACINTOCOUNY] | helldown | Link |
| 2024-11-06 | [brandenburgerplumbing.com] | ransomhub | Link |
| 2024-11-06 | [arcoexc.com] | ransomhub | Link |
| 2024-11-06 | [Lincoln University] | meow | Link |
| 2024-11-06 | [Cape Cod Regional Technical High School (capetech.us)] | fog | Link |
| 2024-11-06 | [GSR Andrade Architects (gsr-andrade.com)] | fog | Link |
| 2024-11-05 | [metroelectric.com] | ransomhub | Link |
| 2024-11-05 | [sector5.ro] | ransomhub | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---------------------------------|-------------------|----------------------|
| 2024-11-05 | [Paragon Plastics] | play | Link |
| 2024-11-05 | [Delfin Design & Manufacturing] | play | Link |
| 2024-11-05 | [Smitty's Supply] | play | Link |
| 2024-11-05 | [S & W Kitchens] | play | Link |
| 2024-11-05 | [Dome Construction] | play | Link |
| 2024-11-06 | [Interoute agency] | lynx | Link |
| 2024-11-06 | [LmayInteroute agency] | lynx | Link |
| 2024-11-05 | [pacificglazing.com] | ransomhub | Link |
| 2024-11-05 | [nwhealthporter.com] | ransomhub | Link |
| 2024-11-05 | [wexfordcounty.org] | embargo | Link |
| 2024-11-05 | [ebrso] | qilin | Link |
| 2024-11-05 | [Model Die & Mold] | lynx | Link |
| 2024-11-04 | [mh-m.org] | embargo | Link |
| 2024-11-05 | [Falco Sult] | bianlian | Link |
| 2024-11-05 | [apoyoconsultoria.com] | ransomhub | Link |
| 2024-11-05 | [Webb Institute] | incransom | Link |
| 2024-11-05 | [Fylde Coast Academy Trust] | rhysida | Link |
| 2024-11-04 | [sundt.com] | ransomhub | Link |
| 2024-11-04 | [Memorial Hospital & Manor] | embargo | Link |
| 2024-11-02 | [Scolari] | dragonforce | Link |
| 2024-11-05 | [McMillan Electric Company] | medusa | Link |
| 2024-11-04 | [maxdata.com.br] | ransomhub | Link |
| 2024-11-04 | [goodline.com.au] | ransomhub | Link |
| 2024-11-04 | [kenanasugarcompany.com] | ransomhub | Link |
| 2024-11-04 | [www.schweiker.de] | ransomhub | Link |
| 2024-11-04 | [www.drbutlerandassociates.com] | ransomhub | Link |
| 2024-11-04 | [www.mssupply.com] | ransomhub | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2024-11-04 | [fullfordelectric.com] | ransomhub | Link |
| 2024-11-04 | [College of Business - Tanzania] | hellcat | Link |
| 2024-11-04 | [Ministry of Education - Jordan] | hellcat | Link |
| 2024-11-04 | [Schneider Electric - France] | hellcat | Link |
| 2024-11-04 | [International University of Sarajevo] | medusa | Link |
| 2024-11-04 | [Whitaker Construction Group] | medusa | Link |
| 2024-11-04 | [European External Action Service (EEAS)] | hunters | Link |
| 2024-11-04 | [csucontracting.com] | ransomhub | Link |
| 2024-11-04 | [redphoenixconstruction.com] | ransomhub | Link |
| 2024-11-04 | [Air Specialists Heating & Air Conditioning] | hunters | Link |
| 2024-11-03 | [krigerconstruction.com] | ransomhub | Link |
| 2024-11-03 | [caseconstruction.com] | ransomhub | Link |
| 2024-11-03 | [lambertstonecommercial.com] | ransomhub | Link |
| 2024-11-04 | [Doctor 24x7] | killsec | Link |
| 2024-11-03 | [Hemubo] | hunters | Link |
| 2024-11-03 | [Elad municipality] | handala | Link |
| 2024-11-03 | [Russell Law Firm, LLC] | bianlian | Link |
| 2024-11-03 | [L & B Transport, L.L.C.] | bianlian | Link |
| 2024-11-03 | [guardianhc] | stormous | Link |
| 2024-11-02 | [bravodigitaltrader.co.uk] | ransomhub | Link |
| 2024-11-02 | [SVP Worldwide] | blacksuit | Link |
| 2024-11-02 | [Sumitomo] | killsec | Link |
| 2024-11-01 | [DieTech North America] | qilin | Link |
| 2024-11-01 | [www.fatboysfleetandauto.com] | ransomhub | Link |
| 2024-11-01 | [lighthouseelectric.com] | ransomhub | Link |
| 2024-11-01 | [JS McCarthy Printers] | play | Link |
| 2024-11-01 | [CGR Technologies] | play | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|----------------------------|-------------------|----------------------|
| 2024-11-01 | [lumiplan.com] | cactus | Link |
| 2024-11-01 | [United Sleep Diagnostics] | medusa | Link |
| 2024-11-01 | [eap.gr] | ransomhub | Link |
| 2024-11-01 | [vikurverk.is] | lockbit3 | Link |
| 2024-11-01 | [mirandaproduce.com.ve] | lockbit3 | Link |
| 2024-11-01 | [Cerp Bretagne Nord] | hunters | Link |
| 2024-11-01 | [Hope Valley Recovery] | rhysida | Link |
| 2024-11-01 | [lsst.ac] | cactus | Link |
| 2024-11-01 | [MCNA Dental] | everest | Link |
| 2024-11-01 | [Arctrade] | everest | 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.