
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240508



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 | 19 |
| 5.0.1 2007 hat ☒ angerufen ☒, sie wollen ihre Path Traversal zurück (Und der Drop-box Sign Hack) | 19 |
| 6 Cyberangriffe: (Mai) | 20 |
| 7 Ransomware-Erpressungen: (Mai) | 20 |
| 8 Quellen | 26 |
| 8.1 Quellenverzeichnis | 26 |
| 9 Impressum | 27 |

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

Android-Patchday: Angreifer können Rechte im System ausweiten

Google schließt am Android-Patchday mehrere Lücken, durch die Angreifer ihre Rechte ausweiten können.

- [Link](#)

—

Trend Micro Antivirus One: Codeschmuggel im macOS-Scanner möglich

Trend Micros Antivirus One lässt sich durch eine Schwachstelle unter macOS beliebigen Code unterjubeln. Ein Update steht bereit.

- [Link](#)

—

Sicherheitsupdates: Angreifer können IP-Telefone von Cisco ausspionieren

Admins sollten zeitnah die abgesicherte Firmware für Ciscos IP-Telefone der Serien 6800, 7800 und 8800 installieren.

- [Link](#)

—

CISA warnt: Microsoft Smartscreen- und Gitlab-Sicherheitsleck werden angegriffen

Die US-Cybersicherheitsbehörde CISA hat Angriffe auf eine Lücke im Microsoft Smartscreen und auf eine Gitlab-Schwachstelle gesichtet.

- [Link](#)

—

Sicherheitsupdates: Angreifer können WLAN-Gateways von Aruba kompromittieren

Wichtige Patches schließen mehrere Schwachstellen in Mobility Conductor, Mobility Controllers, WLAN Gateways und SD-WAN Gateways von Aruba.

- [Link](#)

—

Acronis Cyber Protect: Rechteausweitung und Informationsleck möglich

Sicherheitslecks in Acronis Cyber Protect ermöglichen die Ausweitung der Rechte und Informationsabfluss. Updates korrigieren das.

- [Link](#)

—

Qnap schließt NAS-Sicherheitslücken aus Hacker-Wettbewerb Pwn2Own

NAS-Modelle von Qnap sind verwundbar. Nun hat der Hersteller Sicherheitsupdates für das Betriebssystem und Apps veröffentlicht.

- [Link](#)

Sicherheitsupdates: Angreifer können GitLab-Accounts übernehmen

Wichtige Sicherheitsupdates schließen mehrere Sicherheitslücken in GitLab. Der Anbieter rät zu einem zügigen Update.

- [Link](#)

Cross-Site Scripting: Sicherheitslücken in pfSense ermöglichen Admin-Cookieklau

Die Open-Source-Firewall pfSense hat mehrere Löcher, durch die Angreifer eigenen Javascript-Code einschleusen können. Updates sind verfügbar.

- [Link](#)

Cisco: Angreifer platzieren mithilfe neuer 0-Day-Lücke Hintertüren auf Firewalls

Zwei geschickt gestaltete Hintertüren auf Geräten mit Ciscos ASA- und FTD-System überleben Reboots und Systemupdates. Viele Details sind noch unklar.

- [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 | 0.953820000 | 0.993460000 | Link |
| CVE-2023-6895 | 0.901600000 | 0.987710000 | Link |
| CVE-2023-6553 | 0.922860000 | 0.989350000 | Link |
| CVE-2023-5360 | 0.967230000 | 0.996520000 | Link |
| CVE-2023-4966 | 0.966680000 | 0.996340000 | Link |
| CVE-2023-48795 | 0.962250000 | 0.995060000 | Link |
| CVE-2023-47246 | 0.943770000 | 0.991780000 | Link |
| CVE-2023-46805 | 0.965580000 | 0.996060000 | Link |
| CVE-2023-46747 | 0.972430000 | 0.998370000 | Link |
| CVE-2023-46604 | 0.972730000 | 0.998480000 | Link |
| CVE-2023-43177 | 0.964020000 | 0.995580000 | Link |
| CVE-2023-42793 | 0.970940000 | 0.997730000 | Link |
| CVE-2023-39143 | 0.953670000 | 0.993430000 | Link |
| CVE-2023-38646 | 0.913020000 | 0.988530000 | Link |
| CVE-2023-38205 | 0.922000000 | 0.989250000 | Link |
| CVE-2023-38203 | 0.971170000 | 0.997850000 | Link |
| CVE-2023-38035 | 0.974130000 | 0.999300000 | Link |
| CVE-2023-36845 | 0.966630000 | 0.996320000 | Link |
| CVE-2023-3519 | 0.911860000 | 0.988470000 | Link |
| CVE-2023-35082 | 0.959780000 | 0.994560000 | Link |
| CVE-2023-35078 | 0.966030000 | 0.996160000 | Link |
| CVE-2023-34993 | 0.966220000 | 0.996200000 | Link |
| CVE-2023-34960 | 0.934040000 | 0.990620000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-34634 | 0.918830000 | 0.988990000 | Link |
| CVE-2023-34362 | 0.955650000 | 0.993790000 | Link |
| CVE-2023-34039 | 0.934640000 | 0.990670000 | Link |
| CVE-2023-3368 | 0.908410000 | 0.988160000 | Link |
| CVE-2023-33246 | 0.973220000 | 0.998760000 | Link |
| CVE-2023-32315 | 0.974090000 | 0.999260000 | Link |
| CVE-2023-32235 | 0.911650000 | 0.988450000 | Link |
| CVE-2023-30625 | 0.945200000 | 0.992100000 | Link |
| CVE-2023-30013 | 0.960350000 | 0.994670000 | Link |
| CVE-2023-29300 | 0.969500000 | 0.997190000 | Link |
| CVE-2023-29298 | 0.948030000 | 0.992510000 | Link |
| CVE-2023-28771 | 0.914030000 | 0.988610000 | Link |
| CVE-2023-28432 | 0.935270000 | 0.990740000 | Link |
| CVE-2023-28121 | 0.945870000 | 0.992180000 | Link |
| CVE-2023-27524 | 0.970430000 | 0.997530000 | Link |
| CVE-2023-27372 | 0.973780000 | 0.999040000 | Link |
| CVE-2023-27350 | 0.970720000 | 0.997640000 | Link |
| CVE-2023-26469 | 0.942400000 | 0.991580000 | Link |
| CVE-2023-26360 | 0.962720000 | 0.995190000 | Link |
| CVE-2023-26035 | 0.969280000 | 0.997130000 | Link |
| CVE-2023-25717 | 0.957880000 | 0.994200000 | Link |
| CVE-2023-25194 | 0.969190000 | 0.997100000 | Link |
| CVE-2023-2479 | 0.963600000 | 0.995440000 | Link |
| CVE-2023-24489 | 0.974200000 | 0.999330000 | Link |
| CVE-2023-23752 | 0.932080000 | 0.990370000 | Link |
| CVE-2023-23397 | 0.926450000 | 0.989860000 | Link |
| CVE-2023-23333 | 0.963260000 | 0.995340000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|----------------|-------------|-------------|-----------------------|
| CVE-2023-22527 | 0.974360000 | 0.999420000 | Link |
| CVE-2023-22518 | 0.966350000 | 0.996250000 | Link |
| CVE-2023-22515 | 0.972060000 | 0.998190000 | Link |
| CVE-2023-21839 | 0.958250000 | 0.994280000 | Link |
| CVE-2023-21554 | 0.959160000 | 0.994450000 | Link |
| CVE-2023-20887 | 0.963870000 | 0.995540000 | Link |
| CVE-2023-1671 | 0.968860000 | 0.997010000 | Link |
| CVE-2023-0669 | 0.969750000 | 0.997290000 | Link |

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 07 May 2024

[UPDATE] [hoch] Hirschmann HiEOS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] Internet Systems Consortium BIND: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Internet Systems Consortium BIND ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- [Link](#)

—

Tue, 07 May 2024

[NEU] [UNGEPATCHT] [hoch] VPN Clients / DHCP: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in VPN-Clients ausnutzen, die auf DHCP konfigurierten Systemen laufen, um den Datenverkehr umzuleiten.

- [Link](#)

—

Tue, 07 May 2024

[NEU] [hoch] Google Android Patchday Mai 2024: Mehrere Schwachstellen

Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um seine Privilegien zu erhöhen oder vertrauliche Informationen offenlegen.

- [Link](#)

—

Tue, 07 May 2024

[NEU] [UNGEPATCHT] [hoch] Moxa NPort: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Moxa NPort ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] Apache HttpComponents: Schwachstelle ermöglicht Täuschung des Nutzers

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache HttpComponents ausnutzen, um den Nutzer zu täuschen.

- [Link](#)

—

Tue, 07 May 2024

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

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Cross-Site-Scripting-Angriff durchzuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen, Dateien zu manipulieren und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht nicht spezifizierten Angriff

Ein Angreifer kann eine Schwachstelle in xpdf ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] xpdf: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in xpdf ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [kritisch] Microsoft Windows und Microsoft Windows Server: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und seine Privilegien zu erweitern

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen.

- [Link](#)

—

Tue, 07 May 2024

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

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

- [Link](#)

—

Tue, 07 May 2024

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

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

- [Link](#)

—

Tue, 07 May 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] Podman: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- [Link](#)

—

Tue, 07 May 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](#)

—

Tue, 07 May 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Tue, 07 May 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](#)

—

Mon, 06 May 2024

[NEU] [UNGEPATCHT] [kritisch] Linksys Router: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Linksys Router ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|----------|------------------------------------------------------------------------------------------------------|-----------|
| 5/7/2024 | [SUSE SLES15 / openSUSE 15 Security Update : SUSE Manager Client Tools (SUSE-SU-2024:1509-1)] | critical |
| 5/7/2024 | [Google Chrome < 124.0.6367.155 Multiple Vulnerabilities] | critical |
| 5/7/2024 | [GLSA-202405-18 : Xpdf: Multiple Vulnerabilities] | high |
| 5/7/2024 | [GLSA-202405-20 : libjpeg-turbo: Multiple Vulnerabilities] | high |
| 5/7/2024 | [SUSE SLES15 Security Update : kernel RT (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2024:1491-1)] | high |
| 5/7/2024 | [SUSE SLES15 Security Update : SUSE Manager Server 4.3 (SUSE-SU-2024:1532-1)] | high |
| 5/7/2024 | [SUSE SLES15 Security Update : flatpak (SUSE-SU-2024:1535-1)] | high |
| 5/7/2024 | [SUSE SLES12 / SLES15 Security Update : kernel (Live Patch 42 for SLE 15 SP2) (SUSE-SU-2024:1493-1)] | high |
| 5/7/2024 | [SUSE SLES12 Security Update : kernel (Live Patch 42 for SLE 12 SP5) (SUSE-SU-2024:1505-1)] | high |
| 5/7/2024 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : flatpak (SUSE-SU-2024:1536-1)] | high |
| 5/7/2024 | [SUSE SLES15 Security Update : less (SUSE-SU-2024:1534-1)] | high |
| 5/7/2024 | [SUSE SLES15 Security Update : SUSE Manager Salt Bundle (SUSE-SU-2024:1518-1)] | high |
| 5/7/2024 | [SUSE SLES15 Security Update : SUSE Manager Server 4.3 (SUSE-SU-2024:1507-1)] | high |
| 5/7/2024 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : skopeo (SUSE-SU-2024:1497-1)] | high |

| Datum | Schwachstelle | Bewertung |
|----------|---------------------------------------------------------------------------------------------|-----------|
| 5/7/2024 | [SUSE SLES15 Security Update : kernel (Live Patch 44 for SLE 15 SP2) (SUSE-SU-2024:1506-1)] | high |
| 5/7/2024 | [Fedora 40 : nano (2024-93f31f5de6)] | high |
| 5/7/2024 | [Fedora 40 : webkit2gtk4.0 (2024-a1246372a4)] | high |
| 5/7/2024 | [Oracle Linux 6 / 7 : Unbreakable Enterprise kernel (ELSA-2024-12354)] | high |
| 5/7/2024 | [RHEL 8 : glibc (RHSA-2024:2722)] | high |
| 5/7/2024 | [RHEL 8 : bind and dhcp (RHSA-2024:2721)] | high |
| 5/7/2024 | [RHEL 8 / 9 : Red Hat JBoss Web Server 6.0.2 (RHSA-2024:1916)] | high |
| 5/7/2024 | [RHEL 7 / 8 / 9 : Red Hat JBoss Web Server 5.8.0 (RHSA-2024:1913)] | high |
| 5/7/2024 | [Ubuntu 22.04 LTS : Linux kernel (OEM) vulnerabilities (USN-6765-1)] | high |
| 5/7/2024 | [Oracle Linux 9 : tigervnc (ELSA-2024-2616)] | high |
| 5/7/2024 | [F5 Networks BIG-IP : Node.js vulnerability (K000139532)] | high |
| 5/7/2024 | [Oracle Linux 9 : libxml2 (ELSA-2024-2679)] | high |
| 5/7/2024 | [Oracle Linux 9 : podman (ELSA-2024-2548)] | high |
| 5/7/2024 | [Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6766-1)] | high |
| 5/7/2024 | [Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6767-1)] | high |
| 5/6/2024 | [Zebra Industrial Printers Insufficiently Protected Credentials (CVE-2019-10960)] | high |

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 06 May 2024

Systemd Insecure PTY Handling

Systemd-run/run0 allocates user-owned ptys and attaches the slave to high privilege programs without changing ownership or locking the pty slave.

- [Link](#)

—

” “Mon, 06 May 2024

Microsoft PlayReady Toolkit

The Microsoft PlayReady toolkit assists with fake client device identity generation, acquisition of license and content keys for encrypted content, and much more. It demonstrates weak content protection in the environment of CANAL+. The proof of concept exploit 3 year old vulnerabilities in CANAL+ STB devices, which make it possible to gain code execution access to target STB devices over an IP network.

- [Link](#)

—

” “Mon, 06 May 2024

Docker Privileged Container Kernel Escape

This Metasploit module performs a container escape onto the host as the daemon user. It takes advantage of the SYS_MODULE capability. If that exists and the linux headers are available to compile on the target, then we can escape onto the host.

- [Link](#)

—

” “Fri, 03 May 2024

SOPanning 1.52.00 SQL Injection

SOPanning version 1.52.00 suffers from a remote SQL injection vulnerability in projects.php.

- [Link](#)

—

” “Fri, 03 May 2024

SOPanning 1.52.00 Cross Site Request Forgery

SOPanning version 1.52.00 suffers from a cross site request forgery vulnerability in xajax_server.php.

- [Link](#)

—

” “Fri, 03 May 2024

SOPanning 1.52.00 Cross Site Scripting

SOPlanning version 1.52.00 suffers from a cross site scripting vulnerability in groupe_save.php.

- [Link](#)

—

” “Thu, 02 May 2024

htmlLawed 1.2.5 Remote Command Execution

htmlLawed versions 1.2.5 and below proof of concept remote command execution exploit.

- [Link](#)

—

” “Wed, 01 May 2024

Packet Storm New Exploits For April, 2024

This archive contains all of the 132 exploits added to Packet Storm in April, 2024.

- [Link](#)

—

” “Wed, 01 May 2024

Online Tours And Travels Management System 1.0 SQL Injection

Online Tours and Travels Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 30 Apr 2024

Windows PspBuildCreateProcessContext Double-Fetch / Buffer Overflow

Proof of concept code that demonstrates how the Windows kernel suffers from a privilege escalation vulnerability due to a double-fetch in PspBuildCreateProcessContext that leads to a stack buffer overflow.

- [Link](#)

—

” “Tue, 30 Apr 2024

Windows NtQueryInformationThread Double-Fetch / Arbitrary Write

Proof of concept code that demonstrates how the Windows kernel suffers from a privilege escalation vulnerability due to a double-fetch in NtQueryInformationThread that leads to an arbitrary write.

- [Link](#)

—

” “Tue, 30 Apr 2024

undefinedExploiting The NT Kernel In 24H2undefined

This is the full Windows privilege escalation exploit produced from the blog Exploiting the NT Kernel in 24H2: New Bugs in Old Code and Side Channels Against KASLR.

- [Link](#)

—

” “Tue, 30 Apr 2024

osCommerce 4 Cross Site Scripting

osCommerce version 4 suffers from a cross site scripting vulnerability. This finding is another vector of attack for this issue already discovered by the same researcher in November of 2023.

- [Link](#)

—

” “Mon, 29 Apr 2024

Kemp LoadMaster Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Kemp LoadMaster in the authorization header after version 7.2.48.1. The following versions are patched: 7.2.59.2 (GA), 7.2.54.8 (LTSF), and 7.2.48.10 (LTS).

- [Link](#)

—

” “Mon, 29 Apr 2024

Doctor Appointment Management System 1.0 Cross Site Scripting

Doctor Appointment Management System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 29 Apr 2024

ESET NOD32 Antivirus 17.1.11.0 Unquoted Service Path

ESET NOD32 Antivirus version 17.1.11.0 suffers from an unquoted service path vulnerability.

- [Link](#)

—

” “Thu, 25 Apr 2024

PowerVR PMRMMMapPMR() Writability Check

PowerVR has a security issue where a writability check in PMRMMMapPMR() does not clear VM_MAYWRITE.

- [Link](#)

—

” “Wed, 24 Apr 2024

Apache Solr Backup/Restore API Remote Code Execution

Apache Solr versions 6.0.0 through 8.11.2 and versions 9.0.0 up to 9.4.1 are affected by an unrestricted file upload vulnerability which can result in remote code execution in the context of the user running Apache Solr. When Apache Solr creates a Collection, it will use a specific directory as the classpath and load some classes from it. The backup function of the Collection can export malicious class files uploaded by attackers to the directory, allowing Solr to load custom classes and create arbitrary Java code. Execution can further bypass the Java sandbox configured by Solr, ultimately causing arbitrary command execution.

- [Link](#)

—

” “Wed, 24 Apr 2024

Relate Learning And Teaching System SSTI / Remote Code Execution

Relate Learning and Teaching System versions prior to 2024.1 suffers from a server-side template injection vulnerability that leads to remote code execution. This particular finding targets the Batch-Issue Exam Tickets function.

- [Link](#)

—

” “Wed, 24 Apr 2024

Nginx 1.25.5 Host Header Validation

Nginx versions 1.25.5 and below appear to have a host header filtering validation bug that could possibly be used for malice.

- [Link](#)

—

” “Tue, 23 Apr 2024

FortiNet FortiClient EMS 7.2.2 / 7.0.10 SQL Injection / Remote Code Execution

A remote SQL injection vulnerability exists in FortiNet FortiClient EMS (Endpoint Management Server) versions 7.2.0 through 7.2.2 and 7.0.1 through 7.0.10. FortiClient EMS serves as an endpoint management solution tailored for enterprises, offering a centralized platform for overseeing enrolled endpoints. The SQL injection vulnerability is due to user controller strings which can be sent directly into database queries. FcmDaemon.exe is the main service responsible for communicating with enrolled clients. By default it listens on port 8013 and communicates with FCTDas.exe which is responsible for translating requests and sending them to the database. In the message header of a specific request sent between the two services, the FCTUID parameter is vulnerable to SQL injection. It can be used to enable the xp_cmdshell which can then be used to obtain unauthenticated remote code execution in the context of NT AUTHORITY\SYSTEM. Upgrading to either 7.2.3, 7.0.11 or above is recommended by FortiNet. It should be noted that in order to be vulnerable, at least one endpoint needs to be enrolled / managed by FortiClient EMS for the necessary vulnerable services to be available.

- [Link](#)

—

” “Tue, 23 Apr 2024

GitLens Git Local Configuration Execution

GitKraken GitLens versions prior to 14.0.0 allow an untrusted workspace to execute git commands. A repo may include its own .git folder including a malicious config file to execute arbitrary code. Tested against VSCode 1.87.2 with GitLens 13.6.0 on Ubuntu 22.04 and Windows 10.

- [Link](#)

—

” “Tue, 23 Apr 2024

Visual Studio Code Execution

This Metasploit module creates a vsix file which can be installed in Visual Studio Code as an extension. At activation/install, the extension will execute a shell or two. Tested against VSCode 1.87.2 on Ubuntu 22.04.

- [Link](#)

—

” “Tue, 23 Apr 2024

Gambio Online Webshop 4.9.2.0 Remote Code Execution

A remote code execution vulnerability in Gambio online webshop versions 4.9.2.0 and below allows remote attackers to run arbitrary commands via an unauthenticated HTTP POST request. The identified vulnerability within Gambio pertains to an insecure deserialization flaw, which ultimately allows an attacker to execute remote code on affected systems. The insecure deserialization vulnerability in Gambio poses a significant risk to affected systems. As it allows remote code execution, adversaries could exploit this flaw to execute arbitrary commands, potentially resulting in complete system compromise, data exfiltration, or unauthorized access to sensitive information.

- [Link](#)

—

” “Tue, 23 Apr 2024

Palo Alto Networks PAN-OS Unauthenticated Remote Code Execution

This Metasploit module exploits two vulnerabilities in Palo Alto Networks PAN-OS that allow an unauthenticated attacker to create arbitrarily named files and execute shell commands. Configuration requirements are PAN-OS with GlobalProtect Gateway or GlobalProtect Portal enabled and telemetry collection on (default). Multiple versions are affected. Payloads may take up to one hour to execute, depending on how often the telemetry service is set to run.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Tue, 07 May 2024

ZDI-24-427: Adobe Acrobat Reader DC AcroForm Out-Of-Bounds Read Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-426: Adobe Acrobat Reader DC AcroForm Use-After-Free Information Disclosure Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-425: Adobe Acrobat Reader DC AcroForm Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-424: Adobe Acrobat Reader DC AcroForm Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-423: Adobe Acrobat Reader DC AcroForm Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-422: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-421: SonicWALL GMS Virtual Appliance ECMClientAuthenticator Hard-Coded Credential Authentication Bypass Vulnerability

- [Link](#)

—

” “Tue, 07 May 2024

ZDI-24-420: SonicWALL GMS Virtual Appliance ECMPolicy XML External Entity Processing Information Disclosure Vulnerability

- [Link](#)

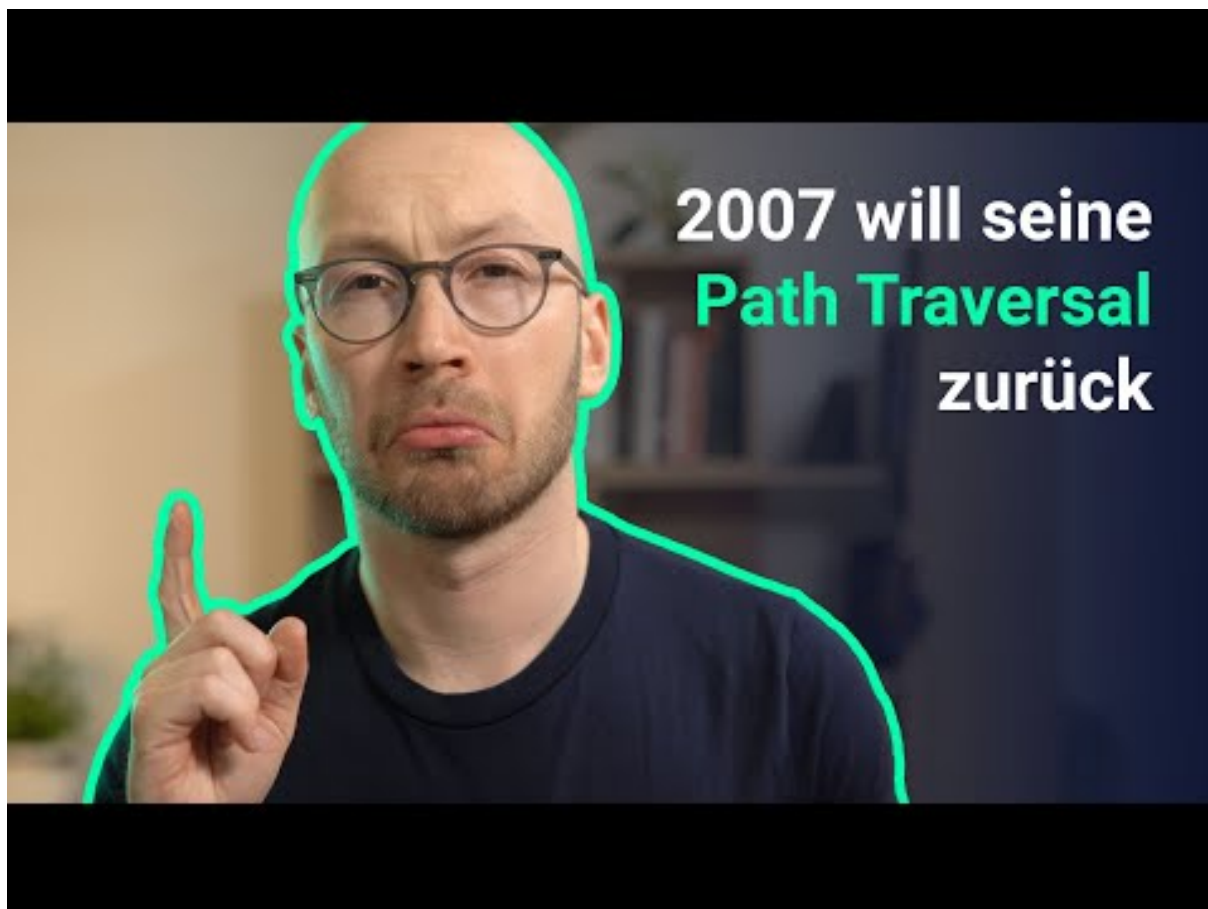
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 2007 hat 0x00000000 angerufen 0x00000000, sie wollen ihre Path Traversal zurück (Und der Dropbox Sign Hack)



[Zum Youtube Video](#)

6 Cyberangriffe: (Mai)

| Datum | Opfer | Land | Information |
|------------|------------------------------|-------|----------------------|
| 2024-05-05 | Wichita | [USA] | Link |
| 2024-05-05 | Université de Sienne | [ITA] | Link |
| 2024-05-04 | Regional Cancer Center (RCC) | [IND] | Link |
| 2024-05-03 | Eucatex (EUCA4) | [BRA] | Link |
| 2024-05-03 | Cégep de Lanaudière | [CAN] | Link |
| 2024-05-03 | Coradix-Magnescan | [FRA] | Link |
| 2024-05-02 | Umeå universitet | [SWE] | Link |

7 Ransomware-Erpressungen: (Mai)

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---------------------------------------------|-------------------|----------------------|
| 2024-05-06 | [Electric Mirror] | incransom | Link |
| 2024-05-07 | [Intuitae] | qilin | Link |
| 2024-05-07 | [Tholen Building Technology Group] | qilin | Link |
| 2024-05-07 | [williamsrdm.com] | qilin | Link |
| 2024-05-07 | [inforius] | qilin | Link |
| 2024-05-07 | [Kamo Jou Trading] | ransomhub | Link |
| 2024-05-07 | [wichita.gov] | lockbit3 | Link |
| 2024-05-01 | [City of Buckeye (buckeyeaz.gov)] | incransom | Link |
| 2024-05-07 | [Hibser Yamauchi Architects] | hunters | Link |
| 2024-05-07 | [Noritsu America Corp.] | hunters | Link |
| 2024-05-07 | [Autohaus Ebert] | metaencryptor | Link |
| 2024-05-07 | [Elbers GmbH & Co. KG] | metaencryptor | Link |
| 2024-05-07 | [Jetson Specialty Marketing Services, Inc.] | metaencryptor | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|----------------------------------------------------------------------|-------------------|----------------------|
| 2024-05-07 | [Vega Reederei GmbH & Co. KG] | metaencryptor | Link |
| 2024-05-07 | [Max Wild GmbH] | metaencryptor | Link |
| 2024-05-07 | [woldae.com] | abyss | Link |
| 2024-05-07 | [Information Integration Experts] | dAn0n | Link |
| 2024-05-06 | [One Toyota of Oakland] | medusa | Link |
| 2024-05-07 | [Chemring Group] | medusa | Link |
| 2024-05-07 | [lalengineering] | ransomhub | Link |
| 2024-05-07 | [skanlog.com] | lockbit3 | Link |
| 2024-05-07 | [ctc-corp.net] | lockbit3 | Link |
| 2024-05-07 | [uslinen.com] | lockbit3 | Link |
| 2024-05-07 | [tu-ilmenau.de] | lockbit3 | Link |
| 2024-05-07 | [thede-culpepper.com] | lockbit3 | Link |
| 2024-05-07 | [kimmelcleaners.com] | lockbit3 | Link |
| 2024-05-07 | [emainc.net] | lockbit3 | Link |
| 2024-05-07 | [southernspecialtysupply.com] | lockbit3 | Link |
| 2024-05-07 | [lenmed.co.za] | lockbit3 | Link |
| 2024-05-07 | [churchill-linen.com] | lockbit3 | Link |
| 2024-05-07 | [rollingfields.com] | lockbit3 | Link |
| 2024-05-07 | [srg-plc.com] | lockbit3 | Link |
| 2024-05-07 | [gorrias-mercedes-benz.fr] | lockbit3 | Link |
| 2024-05-05 | [SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2 Leak] | flocker | Link |
| 2024-05-07 | [Central Florida Equipment] | play | Link |
| 2024-05-07 | [High Performance Services] | play | Link |
| 2024-05-07 | [Mauritzon] | play | Link |
| 2024-05-07 | [Somerville] | play | Link |
| 2024-05-07 | [Donco Air] | play | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---------------------------------------------|-------------------|----------------------|
| 2024-05-07 | [Affordable Payroll & Bookkeeping Services] | play | Link |
| 2024-05-07 | [Utica Mack] | play | Link |
| 2024-05-07 | [KC Scout] | play | Link |
| 2024-05-07 | [Sentry Data Management] | play | Link |
| 2024-05-07 | [aletech.com.br] | darkvault | Link |
| 2024-05-07 | [Young Consulting] | blacksuit | Link |
| 2024-05-06 | [Thaayakam LTD] | ransomhub | Link |
| 2024-05-06 | [The Weinstein Firm] | qilin | Link |
| 2024-05-06 | [Nikolaus & Hohenadel] | bianlian | Link |
| 2024-05-06 | [NRS Healthcare] | ransomhub | Link |
| 2024-05-06 | [gammarenax.ch] | lockbit3 | Link |
| 2024-05-06 | [oraclinical.com] | lockbit3 | Link |
| 2024-05-06 | [acsistemas.com] | lockbit3 | Link |
| 2024-05-06 | [cpashin.com] | lockbit3 | Link |
| 2024-05-06 | [epr-groupe.fr] | lockbit3 | Link |
| 2024-05-06 | [isee.biz] | lockbit3 | Link |
| 2024-05-06 | [cdev.gc.ca] | lockbit3 | Link |
| 2024-05-06 | [netspectrum.ca] | lockbit3 | Link |
| 2024-05-06 | [qstartlabs.com] | lockbit3 | Link |
| 2024-05-06 | [syntax-architektur.at] | lockbit3 | Link |
| 2024-05-06 | [carespring.com] | lockbit3 | Link |
| 2024-05-06 | [grand-indonesia.com] | lockbit3 | Link |
| 2024-05-06 | [remagroup.com] | lockbit3 | Link |
| 2024-05-06 | [telekom.com] | lockbit3 | Link |
| 2024-05-06 | [aev-iledefrance.fr] | lockbit3 | Link |
| 2024-05-06 | [elarabygroup.com] | lockbit3 | Link |
| 2024-05-06 | [thebiglifegroup.com] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------------------------------------------|-------------------|----------------------|
| 2024-05-06 | [sonoco.com] | lockbit3 | Link |
| 2024-05-06 | [ville-bouchemaine.fr] | lockbit3 | Link |
| 2024-05-06 | [eskarabajo.mx] | darkvault | Link |
| 2024-05-06 | [Rafael Viñoly Architects] | blacksuit | Link |
| 2024-05-06 | [TRC Talent Solutions] | blacksuit | Link |
| 2024-05-06 | [M2E Consulting Engineers] | akira | Link |
| 2024-05-06 | [sunray.com] | lockbit3 | Link |
| 2024-05-06 | [eviivo.com] | lockbit3 | Link |
| 2024-05-06 | [kras.hr] | lockbit3 | Link |
| 2024-05-06 | [tdt.aero] | lockbit3 | Link |
| 2024-05-06 | [svenskakyrkan.se] | lockbit3 | Link |
| 2024-05-06 | [htcinc.com] | lockbit3 | Link |
| 2024-05-06 | [irc.be] | lockbit3 | Link |
| 2024-05-06 | [geotechenv.com] | lockbit3 | Link |
| 2024-05-06 | [ishoppes.com] | lockbit3 | Link |
| 2024-05-06 | [parat-technology.com] | lockbit3 | Link |
| 2024-05-06 | [getcloudapp.com] | lockbit3 | Link |
| 2024-05-06 | [yucatan.gob.mx] | lockbit3 | Link |
| 2024-05-06 | [arcus.pl] | lockbit3 | Link |
| 2024-05-06 | [Nestoil] | blacksuit | Link |
| 2024-05-06 | [Patterson & Rothwell Ltd] | medusa | Link |
| 2024-05-06 | [Boyden] | medusa | Link |
| 2024-05-06 | [W.F. Whelan] | medusa | Link |
| 2024-05-05 | [SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2] | flocker | Link |
| 2024-05-05 | [Seneca Nation Health System] | incransom | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-------------------------------------------------------------------------------|-------------------|----------------------|
| 2024-05-05 | [SBC Global, Bitfinex, Coinmom, and Rutgers University Part 2] | flocker | Link |
| 2024-05-04 | [COMPEXLEGAL.COM] | clop | Link |
| 2024-05-04 | [ikfhomefinance.com] | darkvault | Link |
| 2024-05-04 | [The Islamic Emirat of Afghanistan National Environmental Protection Agency] | ransomhub | Link |
| 2024-05-04 | [Accounting Professionals LLC. Price, Breazeale & Chastang] | everest | Link |
| 2024-05-04 | [cmactrans.com] | blackbasta | Link |
| 2024-05-04 | [ids-michigan.com] | blackbasta | Link |
| 2024-05-04 | [provencherroy.ca] | blackbasta | Link |
| 2024-05-04 | [swisspro.ch] | blackbasta | Link |
| 2024-05-04 | [olsonsteel.com] | blackbasta | Link |
| 2024-05-04 | [teaspa.it] | blackbasta | Link |
| 2024-05-04 | [ayesa.com] | blackbasta | Link |
| 2024-05-04 | [synlab.com] | blackbasta | Link |
| 2024-05-04 | [active-pcb.com] | blackbasta | Link |
| 2024-05-04 | [gai-it.com] | blackbasta | Link |
| 2024-05-04 | [Macildowie Associates] | medusa | Link |
| 2024-05-03 | [Dr Charles A Evans] | qilin | Link |
| 2024-05-03 | [Universidad Nacional Autónoma de México] | ransomhub | Link |
| 2024-05-03 | [thelawrencegroup.com] | blackbasta | Link |
| 2024-05-02 | [sharik] | stormous | Link |
| 2024-05-02 | [tdra] | stormous | Link |
| 2024-05-02 | [fanr.gov.ae] | stormous | Link |
| 2024-05-02 | [Bayanat] | stormous | Link |
| 2024-05-02 | [kidx] | stormous | Link |
| 2024-05-03 | [MCS] | qilin | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------------------|-------------------|----------------------|
| 2024-05-03 | [Tohlen Building Technology Group] | qilin | Link |
| 2024-05-03 | [Stainless Foundry & Engineering] | play | Link |
| 2024-05-02 | [Ayoub & associates CPA Firm] | everest | Link |
| 2024-05-02 | [www.servicepower.com] | apt73 | Link |
| 2024-05-02 | [www.credio.eu] | apt73 | Link |
| 2024-05-02 | [Lopez Hnos] | rhysida | Link |
| 2024-05-02 | [GWF Frankenwein] | raworld | Link |
| 2024-05-02 | [Reederei Jüngerhans] | raworld | Link |
| 2024-05-02 | [extraco.ae] | ransomhub | Link |
| 2024-05-02 | [watergate] | qilin | Link |
| 2024-05-02 | [Imedi L] | akira | Link |
| 2024-05-01 | [Azteca Tax Systems] | bianlian | Link |
| 2024-05-01 | [Clinica de Salud del Valle de Salinas] | bianlian | Link |
| 2024-05-01 | [cochraneglobal.com] | underground | Link |
| 2024-05-01 | [UK government] | snatch | Link |
| 2024-05-01 | [hookerfurniture.com] | lockbit3 | Link |
| 2024-05-01 | [alimmigration.com] | lockbit3 | Link |
| 2024-05-01 | [anatomage.com] | lockbit3 | Link |
| 2024-05-01 | [bluegrasstechnologies.net] | lockbit3 | Link |
| 2024-05-01 | [PINNACLEENGR.COM] | clop | Link |
| 2024-05-01 | [MCKINLEYPACKAGING.COM] | clop | Link |
| 2024-05-01 | [PILOTPEN.COM] | clop | Link |
| 2024-05-01 | [colonial.edu] | lockbit3 | Link |
| 2024-05-01 | [cordish.com] | lockbit3 | Link |
| 2024-05-01 | [concorr.com] | lockbit3 | Link |
| 2024-05-01 | [yupousa.com] | lockbit3 | Link |
| 2024-05-01 | [peaseinc.com] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-------------------|-------------------|----------|
| 2024-05-01 | [bdcm.com] | blackbasta | Link |
| 2024-05-01 | [MORTON WILLIAMS] | everest | Link |
| 2024-05-03 | [melting-mind.de] | apt73 | Link |
| 2024-05-21 | [netscout.com] | dispossessor | 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.