# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240521

# Inhaltsverzeichnis

# 1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

# 2 Security-News

## 2.1 Heise - Security-Alert

***Trellix ePolicy Orchestrator ermöglicht Rechteausweitung***

Vor zwei Sicherheitslücken in ePolicy Orchestrator warnt Hersteller Trellix. Bösartige Akteure können ihre Rechte ausweiten.

- Link

—

***Patchday: Intel schließt unter anderem kritische Lücke mit Höchstwertung***

Der Chiphersteller löst mehrere Sicherheitsprobleme in verschiedenen Produkten. Betroffen sind etwa die UEFI-Firmware von Servern und ein KI-Tool.

- Link

—

***Freies Admin-Panel: Codeschmuggel durch Cross-Site-Scripting in Froxlor***

Dank schludriger Eingabefilterung können Angreifer ohne Anmeldung Javascript im Browser des Server-Admins ausführen. Ein Patch steht bereit.

- Link

—

***Access Points von Aruba verwundbar – keine Updates für ältere Versionen***

Aufgrund von mehreren Sicherheitslücken in ArubaOS und InstantOS sind Schadcode-Attacken auf Aruba-Geräte möglich.

- Link

—

***Netzwerksicherheit: Diverse Fortinet-Produkte für verschiedene Attacken anfällig***

Es sind wichtige Sicherheitsupdates für unter anderem FortiSandbox, FortiPortal und FortiWebManager erschienen.

- Link

—

***Cisco: Updates schließen Sicherheitslücken in mehreren Produkten***

In mehreren Cisco-Produkten klaffen Sicherheitslücken, durch die Angreifer sich etwa root-Rechte verschaffen und Geräte kompromittieren können.

- Link

—

***Chrome: Weitere Zero-Day-Lücke mit Update geschlossen***

Zum dritten Mal innerhalb einer Woche aktualisiert Google den Chrome-Webbrowser. Erneut kursiert ein Exploit für eine Zero-Day-Lücke darin.

- Link

—

***LibreOffice: Verklickt – und Malware ausgeführt***

Eine Sicherheitslücke im quelloffenen LibreOffice ermöglicht Angreifern, Opfern Schadcode unterzujubeln. Die müssen nur einmal klicken.

- Link

—

***Firefox und Thunderbird: Verbesserte Funktionen und Sicherheitskorrekturen***

Die neuen Fassungen Firefox 126 und Thunderbird 115.11 schließen Sicherheitslücken. Zudem bringen sie verbesserte Funktionen mit.

- Link

—

***Patchday: Angreifer können Schadcode durch Lücken in Adobe-Software schieben***

Der Softwarehersteller Adobe hat unter anderem Animate, Illustrator und Reader vor möglichen Attacken abgesichert.

- 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 | 0.959520000 | 0.994610000 | Link |
| CVE-2023-6895 | 0.901600000 | 0.987810000 | Link |
| CVE-2023-6553 | 0.909510000 | 0.988380000 | Link |
| CVE-2023-5360 | 0.965120000 | 0.995930000 | Link |
| CVE-2023-4966 | 0.967100000 | 0.996490000 | Link |
| CVE-2023-48795 | 0.962250000 | 0.995160000 | Link |
| CVE-2023-47246 | 0.946220000 | 0.992350000 | Link |
| CVE-2023-46805 | 0.965580000 | 0.996110000 | Link |
| CVE-2023-46747 | 0.970410000 | 0.997570000 | Link |
| CVE-2023-46604 | 0.922790000 | 0.989420000 | Link |
| CVE-2023-43177 | 0.964020000 | 0.995650000 | Link |
| CVE-2023-42793 | 0.970940000 | 0.997780000 | Link |
| CVE-2023-41265 | 0.914120000 | 0.988680000 | Link |
| CVE-2023-39143 | 0.953670000 | 0.993580000 | Link |
| CVE-2023-38646 | 0.913020000 | 0.988630000 | Link |
| CVE-2023-38205 | 0.922000000 | 0.989320000 | Link |
| CVE-2023-38203 | 0.970370000 | 0.997550000 | Link |
| CVE-2023-38035 | 0.974190000 | 0.999320000 | Link |
| CVE-2023-36845 | 0.966630000 | 0.996330000 | Link |
| CVE-2023-3519 | 0.911860000 | 0.988580000 | Link |
| CVE-2023-35082 | 0.967320000 | 0.996580000 | Link |
| CVE-2023-35078 | 0.968250000 | 0.996870000 | Link |
| CVE-2023-34993 | 0.966440000 | 0.996290000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-34960 | 0.933140000 | 0.990660000 | Link |
| CVE-2023-34634 | 0.918830000 | 0.989070000 | Link |
| CVE-2023-34362 | 0.959160000 | 0.994530000 | Link |
| CVE-2023-34039 | 0.935790000 | 0.990920000 | Link |
| CVE-2023-3368 | 0.932830000 | 0.990620000 | Link |
| CVE-2023-33246 | 0.972850000 | 0.998620000 | Link |
| CVE-2023-32315 | 0.974090000 | 0.999260000 | Link |
| CVE-2023-32235 | 0.914550000 | 0.988710000 | Link |
| CVE-2023-30625 | 0.948870000 | 0.992820000 | Link |
| CVE-2023-30013 | 0.963050000 | 0.995370000 | Link |
| CVE-2023-29300 | 0.969500000 | 0.997230000 | Link |
| CVE-2023-29298 | 0.948030000 | 0.992610000 | Link |
| CVE-2023-28771 | 0.914030000 | 0.988680000 | Link |
| CVE-2023-28432 | 0.938730000 | 0.991280000 | Link |
| CVE-2023-28121 | 0.941330000 | 0.991600000 | Link |
| CVE-2023-27524 | 0.970950000 | 0.997790000 | Link |
| CVE-2023-27372 | 0.973760000 | 0.999050000 | Link |
| CVE-2023-27350 | 0.971240000 | 0.997950000 | Link |
| CVE-2023-26469 | 0.942400000 | 0.991730000 | Link |
| CVE-2023-26360 | 0.962980000 | 0.995350000 | Link |
| CVE-2023-26035 | 0.969280000 | 0.997170000 | Link |
| CVE-2023-25717 | 0.956860000 | 0.994110000 | Link |
| CVE-2023-25194 | 0.967170000 | 0.996510000 | Link |
| CVE-2023-2479 | 0.965320000 | 0.996030000 | Link |
| CVE-2023-24489 | 0.974200000 | 0.999330000 | Link |
| CVE-2023-23752 | 0.932080000 | 0.990520000 | Link |
| CVE-2023-23397 | 0.926450000 | 0.989960000 | Link |

| CVE | EPSS | Perzentil | weitere Informationen |
|---|---|---|---|
| CVE-2023-23333 | 0.963260000 | 0.995440000 | Link |
| CVE-2023-22527 | 0.974590000 | 0.999550000 | Link |
| CVE-2023-22518 | 0.962670000 | 0.995260000 | Link |
| CVE-2023-22515 | 0.972310000 | 0.998370000 | Link |
| CVE-2023-21839 | 0.959090000 | 0.994510000 | Link |
| CVE-2023-21554 | 0.959390000 | 0.994600000 | Link |
| CVE-2023-20887 | 0.963500000 | 0.995500000 | Link |
| CVE-2023-1671 | 0.969090000 | 0.997110000 | Link |
| CVE-2023-0669 | 0.969690000 | 0.997280000 | Link |

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

Fri, 17 May 2024

***[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen oder vertrauliche Informationen offenlegen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Trellix ePolicy Orchestrator: Mehrere Schwachstellen***

Ein entfernter authentifizierter Angreifer kann mehrere Schwachstellen in Trellix ePolicy Orchestrator ausnutzen, um seine Rechte zu erweitern oder vertrauliche Informationen offenzulegen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Google Chrome/Microsoft Edge: Schwachstelle ermöglicht nicht spezifizierten Angriff***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome/Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Fri, 17 May 2024

***[NEU] [hoch] Tenable Security Nessus: Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen in Tenable Security Nessus ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.

- Link

—

Fri, 17 May 2024

***[NEU] [hoch] Tenable Security Nessus Agent: Mehrere Schwachstellen ermöglichen Privilegieneskalation***

Ein lokaler Angreifer kann mehrere Schwachstellen in Tenable Security Nessus Agent ausnutzen, um seine Privilegien zu erhöhen oder beliebigen Code auszuführen.

- Link

—

Fri, 17 May 2024

***[NEU] [UNGEPATCHT] [hoch] D-LINK Router: Mehrere Schwachstellen ermöglichen Privilegienerweiterung***

Ein nicht authentifizierter Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen im D-LINK DSL-X1852E Router ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Fri, 17 May 2024

***[NEU] [hoch] IBM FlashSystem: Mehrere Schwachstellen***

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in IBM FlashSystem ausnutzen, um einen Denial of Service Angriff durchzuführen oder um seine Privilegien zu erweitern.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] IBM DB2: Mehrere Schwachstellen***

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in IBM DB2 ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service zu verursachen

- Link

—

Fri, 17 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

—

Fri, 17 May 2024

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

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Logback ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Eclipse Jetty: Mehrere Schwachstellen ermöglichen Denial of Service***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Eclipse Jetty ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Logback: Schwachstelle ermöglicht Denial of Service***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Logback ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Fri, 17 May 2024

***[UPDATE] [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

—

Fri, 17 May 2024

***[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht nicht spezifizierten Angriff***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.
- Link

—

Fri, 17 May 2024

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

Ein entfernter, anonymer 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

—

Fri, 17 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

—

Fri, 17 May 2024

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um Informationen offenzulegen oder um Sicherheitsmaßnahmen zu umgehen.
- Link

—

Fri, 17 May 2024

***[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio und Microsoft .NET Framework ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link

—

### 3.3 Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 5/20/2024 | [SolarWinds ARM < 23.2.4 (arm_2023-2-4)] | critical |
| 5/20/2024 | [TensorFlow < 2.11.1 Multiple Vulnerabilities] | critical |
| 5/20/2024 | [TensorFlow < 2.10.1 Multiple Vulnerabilities] | critical |
| 5/20/2024 | [F5 Networks BIG-IP : Python vulnerabilities (K000139691)] | critical |
| 5/20/2024 | [F5 Networks BIG-IP : Python vulnerabilities (K000139698)] | critical |
| 5/18/2024 | [Fedora 38 : chromium (2024-3a548f46a8)] | critical |
| 5/18/2024 | [Fedora 39 : chromium (2024-382a7dba53)] | critical |
| 5/18/2024 | [FreeBSD : Arti – Security issues related to circuit construction (f393b5a7-1535-11ef-8064-c5610a6efffb)] | critical |
| 5/17/2024 | [CyberPower Power Device Network Utility Missing Authentication (CVE-2024-32735)] | critical |
| 5/20/2024 | [FreeBSD : qt5-webengine – Multiple vulnerabilities (d58455cc-159e-11ef-83d8-4ccc6adda413)] | high |
| 5/20/2024 | [RHEL 9 : firefox (RHSA-2024:2906)] | high |
| 5/20/2024 | [RHEL 9 : thunderbird (RHSA-2024:2903)] | high |
| 5/20/2024 | [RHEL 9 : thunderbird (RHSA-2024:2904)] | high |
| 5/20/2024 | [RHEL 8 : thunderbird (RHSA-2024:2905)] | high |
| 5/20/2024 | [RHEL 9 : nodejs (RHSA-2024:2910)] | high |
| 5/20/2024 | [RHEL 8 : httpd:2.4 (RHSA-2024:2907)] | high |
| 5/20/2024 | [RHEL 8 : thunderbird (RHSA-2024:2911)] | high |
| 5/20/2024 | [RHEL 8 : thunderbird (RHSA-2024:2912)] | high |
| 5/20/2024 | [RHEL 7 : thunderbird (RHSA-2024:2913)] | high |
| 5/20/2024 | [Oracle Solaris Critical Patch Update : apr2024_SRU11_3_36_33_1] | high |
| 5/20/2024 | [Debian dla-3817 : thunderbird - security update] | high |

| Datum | Schwachstelle | Bewertung |
|---|---|---|
| 5/20/2024 | [Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (AWS) vulnerabilities (USN-6766-3)] | high |
| 5/20/2024 | [Ubuntu 14.04 LTS / 16.04 LTS : Linux kernel (Azure) vulnerabilities (USN-6777-2)] | high |
| 5/20/2024 | [RHEL 7 : go-toolset-1.19-golang (RHSA-2024:2892)] | high |
| 5/20/2024 | [Oracle Linux 7 : thunderbird (ELSA-2024-2913)] | high |
| 5/20/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-065)] | high |
| 5/20/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-064)] | high |
| 5/20/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.10-2024-056)] | high |
| 5/20/2024 | [Amazon Linux 2 : kernel (ALASKERNEL-5.15-2024-042)] | high |
| 5/19/2024 | [Fedora 40 : suricata (2024-9cce1f4b49)] | high |
| 5/19/2024 | [Fedora 38 : mingw-python-werkzeug (2024-48123e7aae)] | high |
| 5/19/2024 | [Fedora 39 : buildah (2024-c56e6ff1b5)] | high |
| 5/19/2024 | [Fedora 39 : suricata (2024-aa2fdd75f7)] | high |
| 5/18/2024 | [Fedora 39 : git (2024-4c06645f07)] | high |
| 5/18/2024 | [Fedora 40 : firefox (2024-eabe68b149)] | high |
| 5/18/2024 | [FreeBSD : electron29 – setuid() does not affect libuv’s internal io_uring (a431676c-f86c-4371-b48a-b7d2b0bec3a3)] | high |
| 5/18/2024 | [FreeBSD : OpenSSL – Denial of Service vulnerability (b88aa380-1442-11ef-a490-84a93843eb75)] | high |
| 5/17/2024 | [SAP BusinessObjects Business Intelligence Platform Multiple Vulnerabilities (May 2024)] | high |
| 5/17/2024 | [Debian dsa-5694 : chromium - security update] | high |
| 5/17/2024 | [Debian dsa-5693 : thunderbird - security update] | high |
| 5/17/2024 | [Debian dla-3816 : bind9 - security update] | high |

# 4 Aktiv ausgenutzte Sicherheitslücken

## 4.1 Exploits der letzten 5 Tage

“Mon, 20 May 2024

***Tenant Limited 1.0 SQL Injection***

Tenant Limited version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 20 May 2024

***WordPress XStore Theme 9.3.8 SQL Injection***

WordPress XStore theme version 9.3.8 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 20 May 2024

***Apache OFBiz 18.12.12 Directory Traversal***

Apache OFBiz versions 18.12.12 and below suffer from a directory traversal vulnerability.

- Link

—

” “Mon, 20 May 2024

***Backdrop CMS 1.27.1 Remote Command Execution***

Backdrop CMS version 1.27.1 suffers from a remote command execution vulnerability.

- Link

—

” “Mon, 20 May 2024

***PopojiCMS 2.0.1 Remote Command Execution***

PopojiCMS version 2.0.1 remote command execution exploit that requires an administrative login. This vulnerability was originally reported by tmrswrr in November of 2023.

- Link

—

” “Mon, 20 May 2024

***Rocket LMS 1.9 Cross Site Scripting***

Rocket LMS version 1.9 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Thu, 16 May 2024

***GhostRace: Exploiting And Mitigating Speculative Race Conditions***

This archive is a GhostRace proof of concept exploit exemplifying the concept of a speculative race

condition in a step-by-step single-threaded fashion. Coccinelle scripts are used to scan the Linux kernel version 5.15.83 for Speculative Concurrent Use-After-Free (SCUAF) gadgets.

- Link

—

” “Wed, 15 May 2024

***Cacti 1.2.26 Remote Code Execution***

Cacti versions 1.2.26 and below suffer from a remote code execution execution vulnerability in import.php.

- Link

—

” “Wed, 15 May 2024

***SAP Cloud Connector 2.16.1 Missing Validation***

SAP Cloud Connector versions 2.15.0 through 2.16.1 were found to happily accept self-signed TLS certificates between SCC and SAP BTP.

- Link

—

” “Wed, 15 May 2024

***Zope 5.9 Command Injection***

Zope version 5.9 suffers from a command injection vulnerability in /utilities/mkwsgiinstance.py.

- Link

—

” “Tue, 14 May 2024

***CrushFTP Directory Traversal***

CrushFTP versions prior to 11.1.0 suffers from a directory traversal vulnerability.

- Link

—

” “Tue, 14 May 2024

***TrojanSpy.Win64.EMOTET.A MVID-2024-0684 Code Execution***

TrojanSpy.Win64.EMOTET.A malware suffers from a code execution vulnerability.

- Link

—

” “Tue, 14 May 2024

***Plantronics Hub 3.25.1 Arbitrary File Read***

Plantronics Hub version 3.25.1 suffers from an arbitrary file read vulnerability.

- Link

—

” “Tue, 14 May 2024

***Backdoor.Win32.AsyncRat MVID-2024-0683 Code Execution***

Backdoor.Win32.AsyncRat malware suffers from a code execution vulnerability.

- Link

—

” “Tue, 14 May 2024

***Apache mod_proxy_cluster Cross Site Scripting***

Apache mod_proxy_cluster suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 14 May 2024

***Chyrp 2.5.2 Cross Site Scripting***

Chryp version 2.5.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 14 May 2024

***Leafpub 1.1.9 Cross Site Scripting***

Leafpub version 1.1.9 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 14 May 2024

***Prison Management System Using PHP SQL Injection***

Prison Management System Using PHP suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Mon, 13 May 2024

***Kemp LoadMaster Local sudo Privilege Escalation***

This Metasploit module abuses a feature of the sudo command on Progress Kemp LoadMaster. Certain binary files are allowed to automatically elevate with the sudo command. This is based off of the file name. Some files have this permission are not write-protected from the default bal user. As such, if the file is overwritten with an arbitrary file, it will still auto-elevate. This module overwrites the /bin/loadkeys file with another executable.

- Link

—

” “Mon, 13 May 2024

***Panel.SmokeLoader MVID-2024-0682 Cross Site Request Forgery / Cross Site Scripting***

Panel.SmokeLoader malware suffers from cross site request forgery, and cross site scripting vulnerabilities.

- Link

—

” “Mon, 13 May 2024

***Panel.SmokeLoader MVID-2024-0681 Cross Site Scripting***

Panel.SmokeLoader malware suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 13 May 2024

***Esteghlal F.C. Cross Site Scripting***

Esteghlal F.C.’s site suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 13 May 2024

***Arm Mali 5th Gen Dangling ATE***

In mmu_insert_pages_no_flush(), when a HUGE_HEAD page is mapped to a 2M aligned GPU address, this is done by creating an Address Translation Entry (ATE) at MIDGARD_MMU_LEVEL(2) (in other words, an ATE covering 2M of memory is created). This is wrong because it assumes that at least 2M of memory should be mapped. mmu_insert_pages_no_flush() can be called in cases where less than that should be mapped, for example when creating a short alias of a big native allocation. Later, when kbase_mmu_teardown_pgd_pages() tries to tear down this region, it will detect that unmapping a subsection of a 2M ATE is not possible and write a log message complaining about this, but then proceed as if everything was fine while leaving the ATE intact. This means the higher-level code will proceed to free the referenced physical memory while the ATE still points to it.

- Link

—

” “Thu, 09 May 2024

***Openmediavault Remote Code Execution / Local Privilege Escalation***

Openmediavault versions prior to 7.0.32 have a vulnerability that occurs when users in the web-admin group enter commands on the crontab by selecting the root shell. As a result of exploiting the vulnerability, authenticated web-admin users can run commands with root privileges and receive reverse shell connections.

- Link

—

” “Thu, 09 May 2024

***RIOT 2024.01 Buffer Overflows / Lack Of Size Checks / Out-Of-Bound Access***

RIOT versions 2024.01 and below suffers from multiple buffer overflows, ineffective size checks, and out-of-bounds memory access vulnerabilities.

- Link

—

”

## 4.2 0-Days der letzten 5 Tage

“Sun, 19 May 2024

***ZDI-24-483: Adobe Acrobat Reader DC PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-482: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-481: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-480: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-479: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-478: Adobe Acrobat Reader DC Annotation Use-After-Free Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-477: Adobe Acrobat Reader DC PDF File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-476: (Pwn2Own) QNAP TS-464 HLS_tmp Directory Traversal Arbitrary File Creation Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-475: (Pwn2Own) QNAP TS-464 File Upload Directory Traversal Arbitrary File Creation Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-474: (Pwn2Own) QNAP TS-464 Exposed Dangerous Method Privilege Escalation Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-473: (Pwn2Own) QNAP TS-464 Authentication Service Improper Certificate Validation Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-472: (Pwn2Own) QNAP TS-464 Netmgr Endpoint CRLF Injection Arbitrary Configuration Update Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-471: (Pwn2Own) QNAP TS-464 authLogin SQL Injection Remote Code Execution Vulnerability***

- Link

—

” “Sun, 19 May 2024

***ZDI-24-470: (Pwn2Own) QNAP TS-464 QR Code Device CRLF Injection Arbitrary Configuration Change Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-469: Avira Prime Link Following Local Privilege Escalation Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-468: Sante PACS Server PG Patient Query SQL Injection Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-467: GStreamer EXIF Metadata Parsing Integer Overflow Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-466: Siemens Simcenter Femap IGS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-465: Siemens Simcenter Femap IGS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-464: Siemens Simcenter Femap IGS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-463: Siemens Simcenter Femap IGS File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-462: Siemens Simcenter Femap IGS File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-461: Siemens Simcenter Femap IGS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-460: Siemens Simcenter Femap IGS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-459: Siemens Simcenter Femap IGS File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-458: Siemens Simcenter Femap IGS File Parsing Type Confusion Remote Code Execution Vulnerability***

- Link

—

” “Fri, 17 May 2024

***ZDI-24-457: Siemens Simcenter Femap IGS File Parsing Memory Corruption Remote Code Execution Vulnerability***

- Link

—

”

# 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 Private video

Vorschaubild Zum Youtube Video

## 6 Cyberangriffe: (Mai)

| Datum | Opfer | Land | Information |
|---|---|---|---|
| 2024-05-16 | American Radio Relay League (ARRL) | [USA] | Link |
| 2024-05-15 | MediSecure | [AUS] | Link |
| 2024-05-15 | Rockford Public Schools | [USA] | Link |
| 2024-05-15 | Ranzijn | [NLD] | Link |
| 2024-05-15 | Le Collège Ahuntsic | [CAN] | Link |
| 2024-05-15 | Central Contra Costa Transit Authority (County Connection) | [USA] | Link |
| 2024-05-13 | Universidad Complutense de Madrid | [ESP] | Link |
| 2024-05-13 | L'aéroport et l'école de commerce de Pau | [FRA] | Link |
| 2024-05-12 | Christie's | [CHE] | Link |
| 2024-05-12 | Travelite Holdings Ltd. | [SGP] | Link |
| 2024-05-12 | Union Township School District | [USA] | Link |
| 2024-05-08 | Ascension Health | [USA] | Link |
| 2024-05-06 | DocGo | [USA] | Link |
| 2024-05-06 | Key Tronic Corporation | [USA] | Link |
| 2024-05-05 | Wichita | [USA] | Link |
| 2024-05-05 | Université de Sienne | [ITA] | Link |
| 2024-05-05 | Concord Public Schools et Concord-Carlisle Regional School District | [USA] | 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 |
| 2024-05-02 | Ewing Marion Kauffman School | [USA] | Link |
| 2024-05-01 | Brandywine Realty Trust | [USA] | Link |

## 7 Ransomware-Erpressungen: (Mai)

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-21 | [levian.com] | blackbasta | Link |
| 2024-05-21 | [lactanet.ca] | blackbasta | Link |
| 2024-05-21 | [mfgroup.it] | blackbasta | Link |
| 2024-05-21 | [grupocadarso.com] | blackbasta | Link |
| 2024-05-21 | [atlasoil.com] | blackbasta | Link |
| 2024-05-21 | [trugreen.com] | blackbasta | Link |
| 2024-05-20 | [Matadero de Gijón - Biogas energy plant - mataderodegijon.es] | ransomhub | Link |
| 2024-05-20 | [American Clinical Solutions(acslabtest.com)] | ransomhub | Link |
| 2024-05-20 | [ORIUX: Experts in Mobility ] | ransomhub | Link |
| 2024-05-20 | [Jess-link Products] | hunters | Link |
| 2024-05-20 | [MAH Machine] | bianlian | Link |
| 2024-05-20 | [Marigin] | akira | Link |
| 2024-05-20 | [GE Aerospace] | meow | Link |
| 2024-05-20 | [Crooker] | 8base | Link |
| 2024-05-20 | [Embellir] | 8base | Link |
| 2024-05-20 | [LEMKEN] | 8base | Link |
| 2024-05-20 | [California Highway Patrol (SVEL237.org)] | incransom | Link |
| 2024-05-20 | [qualityplumbingassociates.com] | lockbit3 | Link |
| 2024-05-18 | [Regional Obstetrical Consultants] | incransom | Link |
| 2024-05-20 | [Specialty Market Managers] | incransom | Link |
| 2024-05-20 | [Sterling Transportation Services (sts.local)] | incransom | Link |
| 2024-05-20 | [Continuing Healthcare Solutions (chs.local)] | incransom | Link |
| 2024-05-20 | [schuettemetals.com] | cactus | Link |
| 2024-05-07 | [allied-mechanical-services-inc] | incransom | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-16 | [Patriot Machine, Updated data leak.] | donutleaks | Link |
| 2024-05-18 | [carcajou.fr] | lockbit3 | Link |
| 2024-05-18 | [equinoxinc.org] | lockbit3 | Link |
| 2024-05-18 | [unisi.it] | lockbit3 | Link |
| 2024-05-18 | [Widdop & Co.] | rhysida | Link |
| 2024-05-18 | [Colégio Nova Dimensão] | arcusmedia | Link |
| 2024-05-18 | [catiglass.com $100.000] | blacksuit | Link |
| 2024-05-18 | [Bluebonnet Nutrition] | bianlian | Link |
| 2024-05-18 | [Center for Digestive Health] | bianlian | Link |
| 2024-05-18 | [drmsusa.com] | incransom | Link |
| 2024-05-17 | [WEICON] | medusa | Link |
| 2024-05-17 | [County Connection] | medusa | Link |
| 2024-05-17 | [Elm Grove] | medusa | Link |
| 2024-05-17 | [Comwave ] | medusa | Link |
| 2024-05-17 | [Mesopolys] | spacebears | Link |
| 2024-05-14 | [Pittsburgh’s Trusted Orthopaedic Surgeons] | donutleaks | Link |
| 2024-05-17 | [Sullairargentina.com] | redransomware | Link |
| 2024-05-15 | [www.belcherpharma.com] | underground | Link |
| 2024-05-17 | [orga-soft.de] | embargo | Link |
| 2024-05-17 | [Houston Waste Solutions ] | ransomhub | Link |
| 2024-05-17 | [Shyang Shin Bao Ind. Co., Ltd. (hereinafter referred to as ‘’SSB’’)] | qilin | Link |
| 2024-05-17 | [Vision Mechanical] | blacksuit | Link |
| 2024-05-08 | [aharvey.nf.ca] | incransom | Link |
| 2024-05-17 | [PRIMARYSYS.COM] | clop | Link |
| 2024-05-17 | [Formosa Plastics USA] | hunters | Link |
| 2024-05-16 | [Dean Lumber & Supply] | dragonforce | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-16 | [WindCom] | dragonforce | Link |
| 2024-05-17 | [For sale. Contact through admin. $100.000] | blacksuit | Link |
| 2024-05-17 | [agranibank.org] | killsec | Link |
| 2024-05-17 | [laxmicapital.com.np] | killsec | Link |
| 2024-05-16 | [pricemodern.com] | lockbit3 | Link |
| 2024-05-16 | [OKUANT - okuant.com] | ransomhub | Link |
| 2024-05-16 | [valleyjoist.com] | lockbit3 | Link |
| 2024-05-16 | [fulcrum.pro] | cactus | Link |
| 2024-05-16 | [Insurance Agency Marketing Services] | moneymessage | Link |
| 2024-05-15 | [Neovia] | snatch | Link |
| 2024-05-16 | [Baeckerei-raddatz.de] | cloak | Link |
| 2024-05-14 | [Colonial Surety Company ] | medusa | Link |
| 2024-05-16 | [kauffmanschool.org] | lockbit3 | Link |
| 2024-05-16 | [ema-eda.com] | lockbit3 | Link |
| 2024-05-16 | [twpunionschools.org] | lockbit3 | Link |
| 2024-05-16 | [Chuo System Service Co.,Ltd ] | ransomhub | Link |
| 2024-05-16 | [East Shore Sound] | ransomhub | Link |
| 2024-05-16 | [thermalsolutionsllc.com] | threeam | Link |
| 2024-05-16 | [escriba.com.br] | threeam | Link |
| 2024-05-16 | [RIO TECHNOLOGY] | arcusmedia | Link |
| 2024-05-16 | [Egyptian Sudanese] | arcusmedia | Link |
| 2024-05-15 | [Consulting Radiologists] | qilin | Link |
| 2024-05-15 | [FIAB SpA] | qilin | Link |
| 2024-05-15 | [project sold] | monti | Link |
| 2024-05-14 | [Malone] | dragonforce | Link |
| 2024-05-14 | [Hardings Transport] | dragonforce | Link |
| 2024-05-14 | [Connelly Security Systems] | dragonforce | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-14 | [Motor Munich] | dragonforce | Link |
| 2024-05-15 | [epsd.org] | lockbit3 | Link |
| 2024-05-15 | [district70.org] | lockbit3 | Link |
| 2024-05-15 | [keuka.edu] | lockbit3 | Link |
| 2024-05-15 | [allcare-med.com] | lockbit3 | Link |
| 2024-05-15 | [Coplosa] | 8base | Link |
| 2024-05-15 | [Surrey Place Healthcare & Rehabilitation] | rhysida | Link |
| 2024-05-15 | [daubertchemical.com] | lockbit3 | Link |
| 2024-05-08 | [BRAZIL GOV] | arcusmedia | Link |
| 2024-05-11 | [Braz Assessoria Contábil] | arcusmedia | Link |
| 2024-05-11 | [Thibabem Atacadista] | arcusmedia | Link |
| 2024-05-11 | [FILSCAP] | arcusmedia | Link |
| 2024-05-11 | [Cusat] | arcusmedia | Link |
| 2024-05-11 | [Frigrífico Boa Carne] | arcusmedia | Link |
| 2024-05-11 | [GOLD RH S.A.S] | arcusmedia | Link |
| 2024-05-11 | [Grupo SASMET] | arcusmedia | Link |
| 2024-05-15 | [City of Neodesha] | ransomhub | Link |
| 2024-05-08 | [gravetye-manor] | incransom | Link |
| 2024-05-15 | [Wealth Depot LLC] | everest | Link |
| 2024-05-14 | [morrisgroupint.com] | lockbit3 | Link |
| 2024-05-14 | [pierfoundry.com] | blacksuit | Link |
| 2024-05-14 | [Fiskars Group] | akira | Link |
| 2024-05-14 | [Bruno generators (Italian manufacturing)] | akira | Link |
| 2024-05-14 | [GMJ & Co, Chartered Accountants] | bianlian | Link |
| 2024-05-14 | [Rocky Mountain Sales ] | ransomhub | Link |
| 2024-05-14 | [Talley Group] | incransom | Link |
| 2024-05-14 | [acla.de] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-14 | [Watt Carmichael] | dragonforce | Link |
| 2024-05-14 | [500gb/www.confins.com.br/10kk/BR/Come to chat or we will attack you again.] | ransomhub | Link |
| 2024-05-14 | [eucatex.com.br] | ransomhub | Link |
| 2024-05-14 | [LPDB KUMKM LPDB.ID/LPDB.GO.ID] | ransomhub | Link |
| 2024-05-13 | [Accurate Lock and Hardware] | dragonforce | Link |
| 2024-05-13 | [Monocon International Refractory] | dragonforce | Link |
| 2024-05-13 | [Persyn] | dragonforce | Link |
| 2024-05-13 | [Aero Tec Laboratories] | hunters | Link |
| 2024-05-13 | [Altipal] | dragonforce | Link |
| 2024-05-13 | [Municipalité La Guadeloupe] | qilin | Link |
| 2024-05-13 | [Eden Project Ltd] | incransom | Link |
| 2024-05-13 | [Helapet Ltd] | incransom | Link |
| 2024-05-13 | [oseranhahn.com] | lockbit3 | Link |
| 2024-05-13 | [jmjcorporation.com] | lockbit3 | Link |
| 2024-05-13 | [countyins.com] | lockbit3 | Link |
| 2024-05-13 | [utc-silverstone.co.uk] | lockbit3 | Link |
| 2024-05-13 | [hesperiausd.org] | lockbit3 | Link |
| 2024-05-13 | [Eden Project] | incransom | Link |
| 2024-05-13 | [umbrellaproperties.com] | dispossessor | Link |
| 2024-05-13 | [Treasury of Cote d'Ivoire] | hunters | Link |
| 2024-05-13 | [scanda.com.mx] | cactus | Link |
| 2024-05-13 | [acfin.cl] | cactus | Link |
| 2024-05-13 | [New Boston Dental Care] | 8base | Link |
| 2024-05-13 | [Service public de Wallonie] | 8base | Link |
| 2024-05-13 | [Cushman Contracting Corporation] | 8base | Link |
| 2024-05-13 | [Costa Edutainment SpA] | 8base | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-13 | [Sigmund Espeland AS] | 8base | Link |
| 2024-05-13 | [Brovedani Group] | 8base | Link |
| 2024-05-13 | [Fic Expertise] | 8base | Link |
| 2024-05-13 | [W.I.S. Sicherheit] | 8base | Link |
| 2024-05-12 | [Brick Court Chambers] | medusa | Link |
| 2024-05-03 | [Seaman’s Mechanical] | incransom | Link |
| 2024-05-06 | [Deeside Timberframe] | incransom | Link |
| 2024-05-12 | [McSweeney / Langevin] | qilin | Link |
| 2024-05-11 | [NITEK International LLC] | medusa | Link |
| 2024-05-11 | [National Metalwares, L.P] | medusa | Link |
| 2024-05-12 | [Romeo Pitaro Injury & Litigation Lawyers] | bianlian | Link |
| 2024-05-11 | [NHS (press update)] | incransom | Link |
| 2024-05-11 | [Jackson County] | blacksuit | Link |
| 2024-05-11 | [For sale. Contact through admin.] | blacksuit | Link |
| 2024-05-10 | [21stcenturyvitamins.com] | lockbit3 | Link |
| 2024-05-10 | [Montgomery County Board of Developmental Disabilities Services] | blacksuit | Link |
| 2024-05-10 | [LiveHelpNow] | play | Link |
| 2024-05-10 | [NK Parts Industries] | play | Link |
| 2024-05-10 | [Badger Tag & Label] | play | Link |
| 2024-05-10 | [Haumiller Engineering] | play | Link |
| 2024-05-10 | [Barid soft] | stormous | Link |
| 2024-05-10 | [Pella] | hunters | Link |
| 2024-05-10 | [Reading Electric] | akira | Link |
| 2024-05-10 | [Kuhn Rechtsanwlte GmbH] | monti | Link |
| 2024-05-10 | [colonialsd.org] | lockbit3 | Link |
| 2024-05-09 | [wisconsinindustrialcoatings.com] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-09 | [amsoft.cl] | lockbit3 | Link |
| 2024-05-09 | [cultivarnet.com.br] | lockbit3 | Link |
| 2024-05-09 | [ecotruck.com.br] | lockbit3 | Link |
| 2024-05-09 | [iaconnecticut.com] | lockbit3 | Link |
| 2024-05-09 | [incegroup.com] | lockbit3 | Link |
| 2024-05-09 | [contest.omg] | lockbit3 | Link |
| 2024-05-05 | [Banco central argentina] | zerotolerance | Link |
| 2024-05-09 | [Administração do Porto de São Francisco do Sul (APSFS)] | ransomhub | Link |
| 2024-05-09 | [lavalpoincon.com] | lockbit3 | Link |
| 2024-05-09 | [ccimp.com] | lockbit3 | Link |
| 2024-05-09 | [ufresources.com] | lockbit3 | Link |
| 2024-05-09 | [cloudminds.com] | lockbit3 | Link |
| 2024-05-09 | [calvia.com] | lockbit3 | Link |
| 2024-05-09 | [manusa.com] | lockbit3 | Link |
| 2024-05-09 | [habeco.com.vn] | lockbit3 | Link |
| 2024-05-09 | [rehub.ie] | lockbit3 | Link |
| 2024-05-09 | [torrepacheco.es] | lockbit3 | Link |
| 2024-05-09 | [ccofva.com] | lockbit3 | Link |
| 2024-05-09 | [dagma.com.ar] | lockbit3 | Link |
| 2024-05-09 | [Edlong] | qilin | Link |
| 2024-05-09 | [dpkv.cz] | lockbit3 | Link |
| 2024-05-09 | [hetero.com] | lockbit3 | Link |
| 2024-05-09 | [vikrantsprings.com] | lockbit3 | Link |
| 2024-05-09 | [doublehorse.in] | lockbit3 | Link |
| 2024-05-09 | [iitm.ac.in] | lockbit3 | Link |
| 2024-05-09 | [cttxpress.com] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-09 | [garage-cretot.fr] | lockbit3 | Link |
| 2024-05-09 | [hotel-ostella.com] | lockbit3 | Link |
| 2024-05-09 | [vm3fincas.es] | lockbit3 | Link |
| 2024-05-09 | [thaiagri.com] | lockbit3 | Link |
| 2024-05-09 | [tegaindustries.com] | lockbit3 | Link |
| 2024-05-09 | [kioti.com] | lockbit3 | Link |
| 2024-05-09 | [taylorcrane.com] | lockbit3 | Link |
| 2024-05-09 | [grc-c.co.il] | lockbit3 | Link |
| 2024-05-09 | [mogaisrael.com] | lockbit3 | Link |
| 2024-05-09 | [ultragasmexico.com] | lockbit3 | Link |
| 2024-05-09 | [eif.org.na] | lockbit3 | Link |
| 2024-05-09 | [auburnpikapp.org] | lockbit3 | Link |
| 2024-05-09 | [acla-werke.com] | lockbit3 | Link |
| 2024-05-09 | [college-stemarie-elven.org] | lockbit3 | Link |
| 2024-05-09 | [snk.sk] | lockbit3 | Link |
| 2024-05-09 | [mutualclubunion.com.ar] | lockbit3 | Link |
| 2024-05-09 | [rfca.com] | lockbit3 | Link |
| 2024-05-09 | [hpo.pe] | lockbit3 | Link |
| 2024-05-09 | [spu.ac.th] | lockbit3 | Link |
| 2024-05-09 | [livia.in] | lockbit3 | Link |
| 2024-05-09 | [cinealbeniz.com] | lockbit3 | Link |
| 2024-05-09 | [truehomesusa.com] | lockbit3 | Link |
| 2024-05-09 | [uniter.net] | lockbit3 | Link |
| 2024-05-09 | [itss.com.tr] | lockbit3 | Link |
| 2024-05-09 | [elements-ing.com] | lockbit3 | Link |
| 2024-05-09 | [heartlandhealthcenter.org] | lockbit3 | Link |
| 2024-05-09 | [dsglobaltech.com] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-09 | [alian.mx] | lockbit3 | Link |
| 2024-05-09 | [evw.k12.mn.us] | lockbit3 | Link |
| 2024-05-09 | [mpeprevencion.com] | lockbit3 | Link |
| 2024-05-09 | [binder.de] | lockbit3 | Link |
| 2024-05-09 | [interfashion.it] | lockbit3 | Link |
| 2024-05-09 | [vstar.in] | lockbit3 | Link |
| 2024-05-09 | [brfibra.com] | lockbit3 | Link |
| 2024-05-09 | [museu-goeldi.br] | lockbit3 | Link |
| 2024-05-09 | [doxim.com] | lockbit3 | Link |
| 2024-05-09 | [essinc.com] | lockbit3 | Link |
| 2024-05-09 | [sislocar.com] | lockbit3 | Link |
| 2024-05-09 | [depenning.com] | lockbit3 | Link |
| 2024-05-09 | [asafoot.com] | lockbit3 | Link |
| 2024-05-09 | [frankmiller.com] | blacksuit | Link |
| 2024-05-09 | [vitema.vi.gov] | lockbit3 | Link |
| 2024-05-09 | [snapethorpeprimary.co.uk] | lockbit3 | Link |
| 2024-05-09 | [agencavisystems.com] | lockbit3 | Link |
| 2024-05-09 | [salmonesaysen.cl] | lockbit3 | Link |
| 2024-05-09 | [kowessex.co.uk] | lockbit3 | Link |
| 2024-05-09 | [totto.com] | lockbit3 | Link |
| 2024-05-09 | [randi-group.com] | lockbit3 | Link |
| 2024-05-09 | [grupopm.com] | lockbit3 | Link |
| 2024-05-09 | [ondozabal.com] | lockbit3 | Link |
| 2024-05-09 | [orsiniimballaggi.com] | lockbit3 | Link |
| 2024-05-09 | [vinatiorganics.com] | lockbit3 | Link |
| 2024-05-09 | [peninsulacrane.com] | lockbit3 | Link |
| 2024-05-09 | [brockington.leics.sch.uk] | lockbit3 | Link |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 2024-05-09 | [cargotrinidad.com] | lockbit3 | Link |
| 2024-05-02 | [Pinnacle Orthopaedics] | incransom | Link |
| 2024-05-09 | [Protected: HIDE NAME] | medusalocker | Link |
| 2024-05-09 | [Zuber Gardner CPAs] | everest | Link |
| 2024-05-09 | [Corr & Corr] | everest | Link |
| 2024-05-08 | [rexmoore.com] | embargo | Link |
| 2024-05-08 | [Northeast Orthopedics and Sports Medicine] | dAn0n | Link |
| 2024-05-08 | [Glenwood Management] | dAn0n | Link |
| 2024-05-08 | [College Park Industries] | dAn0n | Link |
| 2024-05-08 | [Holstein Association USA] | qilin | Link |
| 2024-05-08 | [Unimed Vales do Taquari e Rio Pardo] | rhysida | Link |
| 2024-05-08 | [Electric Mirror Inc] | incransom | Link |
| 2024-05-08 | [Richelieu Foods] | hunters | Link |
| 2024-05-08 | [Trade-Mark Industrial] | hunters | Link |
| 2024-05-08 | [Dragon Tax and Management INC] | bianlian | Link |
| 2024-05-08 | [Mewborn & DeSelms] | blacksuit | Link |
| 2024-05-07 | [Merritt Properties, LLC] | medusa | Link |
| 2024-05-07 | [Autobell Car Wash, Inc] | medusa | Link |
| 2024-05-08 | [fortify.pro] | apt73 | Link |
| 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 |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 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 |
| 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 |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 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 |
| 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 |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 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 |
| 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-techology.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 |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 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 |
| 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 |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 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 |
| 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 |

| Datum | Opfer | Ransomware-Grupppe | Webseite |
|---|---|---|---|
| 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 |
| 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.