Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240801

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

Keine Sicherheitsupdates in Sicht: Avast Free Antivirus ist verwundbar

Sicherheitsforscher warnen vor Schwachstellen in Avast Free Antivirus und raten aufgrund fehlender Patches von einer Nutzung ab.

- Link

—

Jetzt patchen! Ransomware-Attacken auf VMware ESXi-Server beobachtet

Sicherheitsforscher warnen vor laufenden Attacken auf Systeme mit ESXi-Hypervisor. Darüber gelangen Erpressungstrojaner auf Computer.

- Link

—

Selenium Grid: Unsichere Standardkonfiguration lässt Krypto-Miner passieren

Das Framework für automatisierte Softwaretests Selenium Grid ist in den Standardeinstellungen verwundbar. Das nutzen Angreifer derzeit aus.

- Link

—

Angreifer nutzen Schadcode-Lücke in Acronis Cyber Infrastructure aus

In mehreren aktualisierten Versionen von Acronis Cyber Infrastructure haben die Entwickler eine kritische Lücke geschlossen.

- Link

—

Sicherheitsupdate schützt SolarWinds Platform vor möglichen Attacken

Angreifer können die IT-Verwaltungssoftware SolarWinds Platform attackieren. Die Entwickler haben mehrere Schwachstellen geschlossen.

- Link

—

Sicherheitslücke: Entwickler raten zum zügigen Patchen von Telerik Report Server

Ein wichtiges Sicherheitsupdate schließt eine kritische Lücke in der IT-Management- und Reporting-lösung Telerik Report Server.

- Link

—

Jetzt patchen! Angreifer attackieren Now Platform von ServiceNow

Die Cloud Computing Plattform von ServiceNow ist derzeit im Visier von Angreifern und sie nutzen kritische Sicherheitslücken aus.

- Link

—

Sicherheitsupdates: Aruba EdgeConnect SD-WAN vielfältig attackierbar

Die Entwickler von HPE haben in Arubas SD-WAN-Lösung EdgeConnect mehrere gefährliche Sicherheitslücken geschlossen.

- Link

—

Docker: Alte Sicherheitslücke zur Rechteausweitung wieder aufgetaucht

Eine Schwachstelle in den Autorisierung-Plug-ins hatte Docker 2019 geschlossen. Sie ist aber kurz danach als Regression wieder in die Engine eingeflossen.

- Link

—

Siemens SICAM: Angreifer können Admin-Passwort zurücksetzen

SCADA-Systeme der SICAM-Reihe von Siemens kommen in kritischen Infrastrukturen zum Einsatz. Sicherheitsupdates schließen eine kritische Lücke.

- 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	0.903160000	0.988630000	Link
CVE-2023-6895	0.922010000	0.989990000	Link
CVE-2023-6553	0.937510000	0.991640000	Link
CVE-2023-5360	0.903980000	0.988700000	Link
CVE-2023-52251	0.938200000	0.991730000	Link
CVE-2023-4966	0.971710000	0.998380000	Link
CVE-2023-49103	0.953130000	0.993900000	Link
CVE-2023-48795	0.964660000	0.996150000	Link
CVE-2023-47246	0.957550000	0.994710000	Link
CVE-2023-46805	0.936080000	0.991470000	Link
CVE-2023-46747	0.972730000	0.998770000	Link
CVE-2023-46604	0.961790000	0.995480000	Link
CVE-2023-4542	0.928310000	0.990640000	Link
CVE-2023-43208	0.965360000	0.996410000	Link
CVE-2023-43177	0.965600000	0.996480000	Link
CVE-2023-42793	0.970370000	0.997900000	Link
CVE-2023-41265	0.911110000	0.989170000	Link
CVE-2023-39143	0.941900000	0.992150000	Link
CVE-2023-38646	0.906610000	0.988880000	Link
CVE-2023-38205	0.954590000	0.994180000	Link
CVE-2023-38203	0.966410000	0.996670000	Link
CVE-2023-38146	0.915710000	0.989460000	Link
CVE-2023-38035	0.974400000	0.999580000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-36845	0.964250000	0.996060000	Link
CVE-2023-3519	0.965340000	0.996390000	Link
CVE-2023-35082	0.968030000	0.997170000	Link
CVE-2023-35078	0.970390000	0.997910000	Link
CVE-2023-34993	0.972880000	0.998840000	Link
CVE-2023-34960	0.936550000	0.991530000	Link
CVE-2023-34634	0.930910000	0.990940000	Link
CVE-2023-34468	0.906650000	0.988880000	Link
CVE-2023-34362	0.969450000	0.997570000	Link
CVE-2023-34039	0.944910000	0.992590000	Link
CVE-2023-3368	0.935570000	0.991410000	Link
CVE-2023-33246	0.972610000	0.998710000	Link
CVE-2023-32315	0.973620000	0.999160000	Link
CVE-2023-30625	0.948260000	0.993120000	Link
CVE-2023-30013	0.962790000	0.995700000	Link
CVE-2023-29300	0.968930000	0.997410000	Link
CVE-2023-29298	0.943640000	0.992410000	Link
CVE-2023-28343	0.923780000	0.990200000	Link
CVE-2023-28121	0.909500000	0.989040000	Link
CVE-2023-27524	0.970600000	0.997990000	Link
CVE-2023-27372	0.973190000	0.998990000	Link
CVE-2023-27350	0.969960000	0.997760000	Link
CVE-2023-26469	0.956500000	0.994540000	Link
CVE-2023-26360	0.959350000	0.995010000	Link
CVE-2023-26035	0.967950000	0.997150000	Link
CVE-2023-25717	0.954090000	0.994070000	Link
CVE-2023-25194	0.968820000	0.997390000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-2479	0.963740000	0.995920000	Link
CVE-2023-24489	0.973540000	0.999130000	Link
CVE-2023-23752	0.960260000	0.995180000	Link
CVE-2023-23333	0.959750000	0.995080000	Link
CVE-2023-22527	0.968290000	0.997230000	Link
CVE-2023-22518	0.964890000	0.996210000	Link
CVE-2023-22515	0.973730000	0.999220000	Link
CVE-2023-21839	0.957210000	0.994630000	Link
CVE-2023-21554	0.952830000	0.993830000	Link
CVE-2023-20887	0.970170000	0.997820000	Link
CVE-2023-1698	0.910560000	0.989130000	Link
CVE-2023-1671	0.962480000	0.995620000	Link
CVE-2023-0669	0.969440000	0.997560000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 31 Jul 2024

[UPDATE] [hoch] expat: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 31 Jul 2024

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Wed, 31 Jul 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

—

Wed, 31 Jul 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

—

Wed, 31 Jul 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder um Sicherheitsmaßnahmen zu umgehen.

- Link

—

Wed, 31 Jul 2024

[UPDATE] [hoch] Microsoft SQL Server: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft SQL Server 2019, Microsoft SQL Server 2022 und Microsoft SQL Server (MSSQL) ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 31 Jul 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen ‘Denial of Service’-Zustand zu verursachen.

- Link

—

Wed, 31 Jul 2024

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

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

- Link

—

Wed, 31 Jul 2024

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

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

- Link

—

Wed, 31 Jul 2024

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

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 31 Jul 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

—

Wed, 31 Jul 2024

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Code auszuführen oder einen unspezifischen Angriff durchzuführen.

- Link

—

Wed, 31 Jul 2024

[UPDATE] [hoch] ImageMagick: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 31 Jul 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Wed, 31 Jul 2024

[NEU] [hoch] Broadcom Brocade Switch: Mehrere Schwachstellen

Ein Angreifer aus einem angrenzenden Netzwerk kann mehrere Schwachstellen in Broadcom Brocade

Switch und Broadcom Fabric OS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen und vertrauliche Informationen preiszugeben.
- Link

—

Tue, 30 Jul 2024

[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.
- Link

—

Tue, 30 Jul 2024

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

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

—

Tue, 30 Jul 2024

[NEU] [UNGEPATCHT] [hoch] Avast Antivirus: Mehrere Schwachstellen ermöglichen Privilegieneskalation und Denial of Service

Ein lokaler Angreifer kann mehrere Schwachstellen in Avast Antivirus ausnutzen, um seine Privilegien zu erhöhen und einen Denial-of-Service-Zustand zu erzeugen.
- Link

—

Tue, 30 Jul 2024

[NEU] [hoch] Apple Safari: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple Safari ausnutzen, um einen Denial of Service Angriff durchzuführen, den Benutzer zu täuschen, einen Cross-Site-Scripting-Angriff zu starten und vertrauliche Informationen preiszugeben.
- Link

—

Tue, 30 Jul 2024

[NEU] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code mit Administratorrechten auszuführen, einen Denial-of-Service-Zustand zu erzeugen, Daten zu modifizieren, den Benutzer zu täuschen, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen.
- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/31/2024	[RHEL 7 : freeradius (RHSA-2024:4911)]	critical
7/31/2024	[RHEL 9 : freeradius (RHSA-2024:4912)]	critical
7/31/2024	[Fedora 39 : xdg-desktop-portal-hyprland (2024-295a735fbc)]	critical
7/31/2024	[RHEL 9 : freeradius (RHSA-2024:4935)]	critical
7/31/2024	[RHEL 7 : httpd (RHSA-2024:4938)]	critical
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : freerdp (SUSE-SU-2024:2631-1)]	critical
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-3 (SUSE-SU-2024:2635-1)]	critical
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : libgit2 (SUSE-SU-2024:2619-1)]	critical
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : apache2 (SUSE-SU-2024:2624-1)]	critical
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : git (SUSE-SU-2024:2656-1)]	critical
7/31/2024	[Fedora 40 : chromium (2024-141c438daf)]	high
7/31/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJDK 11 vulnerabilities (USN-6930-1)]	high
7/31/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJDK 21 vulnerabilities (USN-6932-1)]	high
7/31/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJDK 17 vulnerabilities (USN-6931-1)]	high

Datum	Schwachstelle	Bewertung
7/31/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenJDK 8 vulnerabilities (USN-6929-1)]	high
7/31/2024	[RHEL 9 : git-lfs (RHSA-2024:4934)]	high
7/31/2024	[RHEL 8 : git-lfs (RHSA-2024:4933)]	high
7/31/2024	[CentOS 9 : python-setuptools-53.0.0-13.el9]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-dnspython (SUSE-SU-2024:2626-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : java-17-openjdk (SUSE-SU-2024:2628-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xen (SUSE-SU-2024:2654-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gtk3 (SUSE-SU-2024:2661-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : python-dnspython (SUSE-SU-2024:2655-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : p7zip (SUSE-SU-2024:2625-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gtk2 (SUSE-SU-2024:2660-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : bind (SUSE-SU-2024:2636-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gtk3 (SUSE-SU-2024:2633-1)]	high
7/31/2024	[SUSE SLES12 Security Update : orc (SUSE-SU-2024:2643-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : java-11-openjdk (SUSE-SU-2024:2629-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : gtk2 (SUSE-SU-2024:2634-1)]	high
7/31/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : orc (SUSE-SU-2024:2663-1)]	high

Datum	Schwachstelle	Bewertung
7/31/2024	[Panasonic WV-S2231L Camera Denial of Service (CVE-2020-29194)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 31 Jul 2024

OpenMediaVault rpc.php Authenticated Cron Remote Code Execution

OpenMediaVault allows an authenticated user to create cron jobs as root on the system. An attacker can abuse this by sending a POST request via rpc.php to schedule and execute a cron entry that runs arbitrary commands as root on the system. All OpenMediaVault versions including the latest release 7.4.2-2 are vulnerable.

- Link

—

” “Wed, 31 Jul 2024

Readymade Real Estate Script SQL Injection / Cross Site Scripting

Readymade Real Estate Script suffers from remote blind SQL injection and cross site scripting vulnerabilities.

- Link

—

” “Wed, 31 Jul 2024

AMPLE BILLS 1.0 Cross Site Scripting

AMPLE BILLS version 1.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Wed, 31 Jul 2024

Aero CMS 0.0.1 Cross Site Request Forgery

Aero CMS version 0.0.1 suffers from a cross site request forgery vulnerability.

- Link

—

” “Wed, 31 Jul 2024

SchoolPlus LMS 1.0 SQL Injection

SchoolPlus LMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 31 Jul 2024

AccPack Khanepani 1.0 Insecure Direct Object Reference

AccPack Khanepani version 1.0 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Wed, 31 Jul 2024

AccPack Cop 1.0 SQL Injection

AccPack Cop version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Wed, 31 Jul 2024

AccPack Buzz 1.0 Arbitrary File Upload

AccPack Buzz version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 31 Jul 2024

Academy LMS 6.8.1 Cross Site Scripting

Academy LMS version 6.8.1 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 30 Jul 2024

Chuksrio LMS 2.9 Insecure Direct Object Reference

Chuksrio LMS version 2.9 suffers from an insecure direct object reference vulnerability.

- Link

—

” “Tue, 30 Jul 2024

AMPLE BILLS 1.0 Administrative Page Disclosure

AMPLE BILLS version 1.0 appears to suffer from an administrative page disclosure issue.

- Link

—

” “Tue, 30 Jul 2024

SchoolPlus 1.0 Shell Upload

SchoolPlus version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 30 Jul 2024

AccPack Khanepani 1.0 SQL Injection

AccPack Khanepani version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 30 Jul 2024

AccPack Cop CMS 1.0 SQL Injection

AccPack Cop CMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 30 Jul 2024

AccPack Buzz Cop 1.0 Cross Site Request Forgery

AccPack Buzz Cop version 1.0 suffers from a cross site request forgery vulnerability.

- Link

—

” “Mon, 29 Jul 2024

mySCADA MyPRO Authenticated Command Injection

An authenticated command injection vulnerability exists in MyPRO versions 8.28.0 and below from mySCADA. The vulnerability can be exploited by a remote attacker to inject arbitrary operating system commands which will get executed in the context of NT AUTHORITY\SYSTEM.

- Link

—

” “Mon, 29 Jul 2024

Blog Site 1.0 SQL Injection

Blog Site version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 29 Jul 2024

QuickJob 6.1 Insecure Settings

QuickJob version 6.1 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

Prison Management System version 1.0 Insecure Settings

Prison Management System version version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

PowerVR _DevmemXReservationPageAddress() Wrapping Addition Error

PowerVR has an issue where wrapping addition in _DevmemXReservationPageAddress() causes an MMU operation at the wrong address.

- Link

—

” “Mon, 29 Jul 2024

PowerVR DevmemXIntMapPages() / DevmemXIntUnmapPages() Integer Overflows

PowerVR has integer overflows in DevmemXIntMapPages() and DevmemXIntUnmapPages(), exploitable as dangling GPU page table entries.

- Link

—

” “Mon, 29 Jul 2024

PowerVR PMR Physical Memory Handling Flaw

PowerVR PMR allows physical memory to be freed before GPU TLB invalidation.

- Link

—

” “Mon, 29 Jul 2024

Pharmacy Management System 1.0 Insecure Settings

Pharmacy Management System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

Online Payment Hub System 1.0 Insecure Settings

Online Payment Hub System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Mon, 29 Jul 2024

Innue Business Live Chat 2.5 Insecure Settings

Innue Business Live Chat version 2.5 suffers from an ignored default credential vulnerability.

- Link

—

”

4.2 0-Days der letzten 5 Tage

“Wed, 31 Jul 2024

ZDI-24-1040: Apple macOS AppleVADriver Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1039: PaperCut NG web-print-hot-folder Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1038: PaperCut NG pc-web-print Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1037: PDF-XChange Editor PDF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1036: Check Point ZoneAlarm Extreme Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Wed, 31 Jul 2024

ZDI-24-1035: Microsoft Windows NTFS Junction Heap-based Buffer Overflow Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1034: Oracle VirtualBox EHCI USB Controller Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1033: NI FlexLogger Redis Server Incorrect Permission Assignment Information Disclosure

Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1032: NI FlexLogger Redis Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1031: NI VeriStand NIVSPRJ File Parsing Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1030: NI VeriStand VSMODEL File Parsing Directory Traversal Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1029: NI VeriStand DataLoggingServer Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1028: NI VeriStand WaveformStreamingServer Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1027: NI VeriStand ProjectServer OpenTool Exposed Dangerous Method Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1026: NI VeriStand ProjectServer Exposed Dangerous Method Remote Code Execution Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1025: NI VeriStand IFileTransferServer Exposed Dangerous Method Information Disclosure Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1024: NI VeriStand ProjectServer Exposed Dangerous Method Denial-of-Service Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1023: Trend Micro VPN Proxy One Pro Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1022: Trend Micro VPN Proxy One Pro Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Tue, 30 Jul 2024

ZDI-24-1021: Logsign Unified SecOps Platform Directory Traversal Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1020: SolarWinds Access Rights Manager deleteTransferFile Directory Traversal Arbitrary File Deletion and Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1019: (Pwn2Own) Docker Desktop extension-manager Exposed Dangerous Function Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1018: (Pwn2Own) Linux Kernel io_uring Buffer List Race Condition Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1017: (0Day) Panda Security Dome Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1016: (0Day) Panda Security Dome Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1015: (0Day) Panda Security Dome VPN Incorrect Permission Assignment Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1014: (0Day) Panda Security Dome VPN DLL Hijacking Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1013: (0Day) Panda Security Dome Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1012: (0Day) F-Secure Total Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1011: (0Day) VIPRE Advanced Security SBAMSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1010: (0Day) VIPRE Advanced Security Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1009: (0Day) AVG AntiVirus Free icarus Arbitrary File Creation Denial of Service Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1008: (0Day) AVG AntiVirus Free AVGSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1007: (0Day) AVG AntiVirus Free AVGSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1006: (0Day) AVG AntiVirus Free Link Following Denial-of-Service Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1005: (0Day) Avast Free Antivirus AvastSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1004: (0Day) Avast Free Antivirus AvastSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1003: (0Day) Avast Free Antivirus AvastSvc Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1002: (0Day) Avast Cleanup Premium Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1001: (0Day) Avast Cleanup Premium Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-1000: (0Day) Avast Cleanup Premium Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-999: (0Day) Avast Free Antivirus Link Following Denial-of-Service Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-998: KernelCI SAS Token Incorrect Permission Assignment Authentication Bypass Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-997: Linux Kernel CIFS Filesystem Decryption Improper Input Validation Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-996: Linux Kernel ksmbd ACL Inheritance Heap-based Buffer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-995: Linux Kernel Netfilter Conntrack Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-994: Linux Kernel QXL VGA Driver Race Condition Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-993: Microsoft Azure myapiendpoint.developer.azure-api Improper Access Control Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-992: Microsoft Azure VSTS CLI vstscli Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-991: Microsoft Azure Arc Jumpstart Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-990: Microsoft 3D Builder GLB File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-989: Microsoft Azure Container Network Management sbidprod Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-988: Microsoft Azure MQTT azure-iot-sdks-ci Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-987: Microsoft Object Detection Solution Accelerator csaddevamlacr Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-986: Microsoft Azure IoT Edge Dev Tool iotedgetoolscontainerregistry Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-985: Microsoft Azure Service Fabric servicefabricsdkstorage Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-984: Microsoft Word DOC File Parsing Use-After-Free Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-983: Microsoft Azure Go Labs microsoftgoproxy Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-982: Microsoft Azure SQL Workshop azuremlsampleexperiments Uncontrolled Search Path Element Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-981: Microsoft Azure Machine Learning Notebooks azuremlpackages Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-980: Microsoft Azure Machine Learning Forecasting Toolkit azuremlftkrelease Uncontrolled Search Path Element Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-979: Microsoft Office Visio DXF File Parsing Integer Overflow Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-978: Microsoft PC Manager Link Following Local Privilege Escalation Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-977: Microsoft Office Excel XLW File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-976: Microsoft Office PowerPoint GLB File Parsing Memory Corruption Remote Code Execution Vulnerability

- Link

—

” “Mon, 29 Jul 2024

ZDI-24-975: Microsoft Excel FBX File Parsing Use-After-Free Information Disclosure Vulnerability

- Link

—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Wieder mal die Lieferkette: polyfill.io wird verkauft, spielt Schadcode aus.

Zum Youtube Video

6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-07-31	C-Edge Technologies	[IND]	Link
2024-07-30	Industrias Peñoles	[MEX]	Link
2024-07-30	Intendencia de Paysandú	[URY]	Link
2024-07-30	OneBlood	[USA]	Link
2024-07-29	Fabriano	[ITA]	Link
2024-07-25	Summerville	[USA]	Link
2024-07-24	Département des transports routiers de Selangor	[MYS]	Link
2024-07-23	Red Art Games	[FRA]	Link
2024-07-23	Ville de Cold Lake	[CAN]	Link
2024-07-23	Gouvernement brésilien	[BRA]	Link
2024-07-23	Dibulla	[COL]	Link
2024-07-22	Aéroport de Split	[HRV]	Link
2024-07-22	Forest Park	[USA]	Link
2024-07-22	Jefferson County Clerk’s Office	[USA]	Link
2024-07-21	Schneider Hospital	[VIR]	Link
2024-07-20	Melchers	[SGP]	Link
2024-07-19	Le Tribunal supérieur du comté de Los Angeles	[USA]	Link
2024-07-18	Cadastre hellénique	[GRC]	Link
2024-07-18	Casino du Grand Cercle	[FRA]	Link
2024-07-18	Globes	[ISR]	Link
2024-07-18	Ville de Columbus	[USA]	Link
2024-07-18	Wattle Range Council	[AUS]	Link
2024-07-17	Ingemmet	[PER]	Link
2024-07-16	Le Département de Loire-Atlantique	[FRA]	Link

Datum	Opfer	Land	Information
2024-07-16	Les Transports Publics du Chablais (TPC)	[CHE]	Link
2024-07-15	Department of Migrant Workers (DMW)	[PHL]	Link
2024-07-15	Cadre Holdings, Inc.	[USA]	Link
2024-07-14	Metalfrio	[BRA]	Link
2024-07-14	MERB	[DEU]	Link
2024-07-13	AKG	[DEU]	Link
2024-07-12	Sesc Tocantins	[BRA]	Link
2024-07-12	ValeCard	[BRA]	Link
2024-07-11	Allegheny County District Attorney’s Office	[USA]	Link
2024-07-11	Solutions&Co	[FRA]	Link
2024-07-10	Jaboatão dos Guararapes	[BRA]	Link
2024-07-10	Sibanye Stillwater	[ZAF]	Link
2024-07-10	District scolaire de Goshen	[USA]	Link
2024-07-10	Bassett Furniture Industries Inc.	[USA]	Link
2024-07-10	Active Learning Trust	[GBR]	Link
2024-07-10	Oxfam Hong Kong	[HKG]	Link
2024-07-09	Clay County Courthouse	[USA]	Link
2024-07-09	Ville de Mahina	[FRA]	Link
2024-07-07	Frankfurter University of Applied Sciences (UAS)	[DEU]	Link
2024-07-04	La Ville d’Ans	[BEL]	Link
2024-07-04	Alps Alpine	[CHN]	Link
2024-07-03	E.S.E. Salud Yopal	[COL]	Link
2024-07-03	Florida Department of Health	[USA]	Link
2024-07-03	Southwest Tennessee Community College (SWTCC)	[USA]	Link
2024-07-02	Hong Kong Institute of Architects	[HKG]	Link
2024-07-02	Apex	[USA]	Link

Datum	Opfer	Land	Information
2024-07-01	Hiap Seng Industries	[SGP]	Link
2024-07-01	Monroe County government	[USA]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-30	[EBL PARTNERS (construction	interiors), Florida]	spacebears
2024-07-21	[EFRON LAW FIRM]	spacebears	Link
2024-07-31	[wgma.org]	ransomhub	Link
2024-07-31	[biggreenegg.com]	ransomhub	Link
2024-07-31	[nydj.com]	ransomhub	Link
2024-07-31	[www.pharm-int.com]	ransomhub	Link
2024-07-31	[fingersstore.com]	killsec	Link
2024-07-31	[Find Great People]	akira	Link
2024-07-31	[Carlex Glass Luxembourg S.A.]	metaencryptor	Link
2024-07-31	[Durham Manufacturing]	hunters	Link
2024-07-31	[Kleven Construction]	hunters	Link
2024-07-31	[Florence Cement Company, Inc.]	bianlian	Link
2024-07-31	[Sable International.]	bianlian	Link
2024-07-31	[BRASPRESS]	akira	Link
2024-07-31	[www.srmedicalcenter.org]	qilin	Link
2024-07-26	[sandytownshippolice.org]	lockbit3	Link
2024-07-26	[atcdi.com.cn]	lockbit3	Link
2024-07-28	[frilot.com]	lockbit3	Link
2024-07-28	[pbw-india.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-28	[agapefrance.org]	lockbit3	Link
2024-07-28	[ciberviaxesespecial.net]	lockbit3	Link
2024-07-28	[eastern-sales.com]	lockbit3	Link
2024-07-31	[City of Columbus, Ohio]	rhysida	Link
2024-07-30	[St. Thomas Aquinas High School]	medusa	Link
2024-07-27	[Network Communications Group]	qilin	Link
2024-07-30	[verwarmingheyndrickx.be]	ransomhub	Link
2024-07-30	[stb.ro]	killsec	Link
2024-07-30	[chubb-bulleid.co.uk]	cactus	Link
2024-07-30	[leonardssyrups.com]	cactus	Link
2024-07-30	[westernwyomingbeverages.com]	cactus	Link
2024-07-30	[demos.fr]	cactus	Link
2024-07-30	[denkaiamerica.com]	cactus	Link
2024-07-30	[Macadam Europe]	akira	Link
2024-07-30	[Olschewski Davie]	akira	Link
2024-07-29	[Gemicar]	spacebears	Link
2024-07-30	[welevelup.com]	ransomhub	Link
2024-07-30	[www.chsd117.org]	blacksuit	Link
2024-07-30	[udch.in.th]	ransomhub	Link
2024-07-30	[SAGE Publishing]	akira	Link
2024-07-28	[delhihospital.com]	dispossessor	Link
2024-07-29	[qatar.vcu.edu]	dispossessor	Link
2024-07-29	[tursso.com]	dispossessor	Link
2024-07-29	[airedentalarts.com]	dispossessor	Link
2024-07-29	[labor-koblenz.de]	ransomhub	Link
2024-07-29	[Crownlea Group]	hunters	Link
2024-07-29	[The Gill Corporation]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-29	[Priefert]	hunters	Link
2024-07-29	[BASF - Nunhems]	fog	Link
2024-07-12	[American Golf]	medusa	Link
2024-07-27	[Gentlemen Group GmbH]	medusa	Link
2024-07-17	[The Greenhouse People]	lynx	Link
2024-07-17	[True Blue Environmental]	lynx	Link
2024-07-28	[Ascent Group]	raworld	Link
2024-07-28	[zoppo.com]	abyss	Link
2024-07-28	[intrama-bg]	stormous	Link
2024-07-27	[hanoverhill.com]	blacksuit	Link
2024-07-27	[New Jersey City University]	rhysida	Link
2024-07-25	[glnf.fr]	lockbit3	Link
2024-07-27	[Computer Networking Solutions]	rhysida	Link
2024-07-26	[ayurcan]	qilin	Link
2024-07-27	[Kalaswire.com]	cloak	Link
2024-07-26	[Community Care Alliance]	rhysida	Link
2024-07-22	[www.neurologicalinstitute.com]	ransomhub	Link
2024-07-26	[www.whittakersystem.com]	ransomhub	Link
2024-07-26	[www.castelligroup.com]	ransomhub	Link
2024-07-26	[City of Cold Lake]	fog	Link
2024-07-26	[pioneerworldwide.com]	embargo	Link
2024-07-26	[summervillepolice.com]	embargo	Link
2024-07-26	[blankstyle.com]	darkvault	Link
2024-07-26	[Augusta Orthopedic]	bianlian	Link
2024-07-26	[Karvo Companies, Inc.]	bianlian	Link
2024-07-26	[Planet Group International]	ransomexx	Link
2024-07-26	[LITEON]	ransomexx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-26	[Texas Tech University]	meow	Link
2024-07-26	[Global Industry Analysts]	meow	Link
2024-07-26	[Encore]	meow	Link
2024-07-26	[Daikin]	meow	Link
2024-07-26	[Miami Gardens Florida]	meow	Link
2024-07-26	[Nuclep]	meow	Link
2024-07-26	[Andersen Tax]	meow	Link
2024-07-26	[The Physical Medicine Rehabilitation Center]	meow	Link
2024-07-26	[Villarreal and Begum Law Firm]	meow	Link
2024-07-23	[ach.co.th]	ransomhub	Link
2024-07-23	[bpjaguar.com]	ransomhub	Link
2024-07-24	[oficina.oficinadasfinancas.com.br]	ransomhub	Link
2024-07-26	[Innovalve 3TB Data Leak ($300M)]	handala	Link
2024-07-26	[Speed Advisory]	everest	Link
2024-07-25	[mrhme.org]	ransomhub	Link
2024-07-25	[The Computer Merchant]	play	Link
2024-07-25	[Williams Construction]	play	Link
2024-07-25	[Gateway Extrusions]	play	Link
2024-07-25	[Physical & Occupational Therapy Examiners of Texas]	hunters	Link
2024-07-25	[panitchlaw.com]	ransomhub	Link
2024-07-25	[cminsulation.com]	ransomhub	Link
2024-07-25	[baytoti.com]	ransomhub	Link
2024-07-25	[Gendron & Gendron]	play	Link
2024-07-25	[Golden Business Machines]	play	Link
2024-07-25	[Odyssey Fitness Center]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-25	[OfficeOps]	play	Link
2024-07-25	[BK Aerospace]	dragonforce	Link
2024-07-25	[D&K Group, Inc.]	cicada3301	Link
2024-07-25	[Voss Belting & Specialty]	cicada3301	Link
2024-07-25	[Tri-Star Display]	cicada3301	Link
2024-07-25	[NARSTCO]	cicada3301	Link
2024-07-25	[Odessa College]	fog	Link
2024-07-25	[orbinox.com]	madliberator	Link
2024-07-15	[KMLG]	qilin	Link
2024-07-23	[EHS Partnerships]	qilin	Link
2024-07-25	[Environmental DesignInternational]	akira	Link
2024-07-25	[Empereon Constar]	akira	Link
2024-07-17	[Norther n Bedford County School District (nbcsc.org)]	incransom	Link
2024-07-25	[Physical & Occupational Therapy Examiners ofTexas]	hunters	Link
2024-07-25	[CertiCon]	dragonforce	Link
2024-07-25	[SOLOMONUS.COM]	clop	Link
2024-07-25	[Insula Group]	bianlian	Link
2024-07-22	[tccfleet.com]	lockbit3	Link
2024-07-24	[petroassist.co.uk]	lockbit3	Link
2024-07-24	[e21c.co.uk]	lockbit3	Link
2024-07-23	[Owens Valley Career Development Center]	medusa	Link
2024-07-23	[Coffrage LD]	medusa	Link
2024-07-24	[Vivara]	medusa	Link
2024-07-25	[crimsonwinegroup.com]	abyss	Link
2024-07-24	[Stienemann]	spacebears	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-25	[Pojoaque]	blacksuit	Link
2024-07-24	[Kusum Group of Companies]	raworld	Link
2024-07-24	[TheLutheranFoundation]	raworld	Link
2024-07-24	[Melchers Singapore]	raworld	Link
2024-07-20	[Valisana]	ransomhouse	Link
2024-07-24	[simple-solution-systems]	qilin	Link
2024-07-24	[Bunkhouse Group]	bianlian	Link
2024-07-24	[Playa Vista Job Opportunities and Business Services]	bianlian	Link
2024-07-24	[Accelon Technologies Private]	bianlian	Link
2024-07-24	[SKC West]	akira	Link
2024-07-24	[ORBINOX]	madliberator	Link
2024-07-24	[vrd.be]	madliberator	Link
2024-07-24	[Betances Health Center]	hunters	Link
2024-07-23	[BLEnergy]	handala	Link
2024-07-24	[Jack “Designer” Sparrow.]	donutleaks	Link
2024-07-24	[American Acryl]	akira	Link
2024-07-24	[Electroalfa]	akira	Link
2024-07-24	[CALDAN Conveyor]	akira	Link
2024-07-24	[forestparkga.gov]	monti	Link
2024-07-24	[Regas (regasenergy.com)]	monti	Link
2024-07-24	[Dimbleby Funeral Homes]	dragonforce	Link
2024-07-24	[John Gallin & Son]	dragonforce	Link
2024-07-24	[Industrial Bolsera]	donutleaks	Link
2024-07-24	[RhinoCorps]	blacksuit	Link
2024-07-17	[Congoleum]	play	Link
2024-07-23	[sigmacontrol.eu]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-23	[siParadigm]	akira	Link
2024-07-23	[eurovilla.hr]	darkvault	Link
2024-07-23	[Notarkammer Pfalz]	akira	Link
2024-07-23	[Win Systems]	akira	Link
2024-07-20	[www.byzan.com]	ransomhub	Link
2024-07-16	[maingroup]	incransom	Link
2024-07-08	[Cedar Technologies]	medusa	Link
2024-07-12	[American Golf]	medusa	Link
2024-07-15	[Royal Brighton Yacht Club]	medusa	Link
2024-07-15	[ValeCard]	medusa	Link
2024-07-16	[H&H Group]	medusa	Link
2024-07-16	[Jariet Technologies]	medusa	Link
2024-07-22	[Globes]	medusa	Link
2024-07-22	[AA Munro Insurance]	medusa	Link
2024-07-23	[thesourcinggroup.com]	dAn0n	Link
2024-07-23	[LawDepot]	rhysida	Link
2024-07-23	[Association Management Strategies(AAMC.local)]	incransom	Link
2024-07-08	[CIMP.COM]	incransom	Link
2024-07-22	[Wichita State University Campus of Applied Sciences and Technology]	fog	Link
2024-07-22	[memc.com]	blackbasta	Link
2024-07-22	[SH Pension]	everest	Link
2024-07-11	[Sibanye-Stillwater]	ransomhouse	Link
2024-07-22	[Acadian Ambulance (US)]	daixin	Link
2024-07-21	[Sherbrooke Metals]	BrainCipher	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-21	[Apex Global	Big leak outlooks - 2tb.]	BrainCipher
2024-07-21	[Cole Technologies Group]	BrainCipher	Link
2024-07-21	[Family Wealth Advisors Ltd.]	BrainCipher	Link
2024-07-21	[Mars 2 LLC]	BrainCipher	Link
2024-07-21	[KickDown ESET company. No overpayments at 0% (renamed and update)]	donutleaks	Link
2024-07-21	[Handala’s attack on Israeli organizations]	handala	Link
2024-07-20	[Queens County Public Administrator]	rhysida	Link
2024-07-20	[www.garudafood.com]	ransomhub	Link
2024-07-20	[Reward Hospitality from EFC Group]	blacksuit	Link
2024-07-20	[ESET. PREMIUM.]	donutleaks	Link
2024-07-20	[Doodle Tech]	arcusmedia	Link
2024-07-19	[www.kumagaigumi.co.jp]	ransomhub	Link
2024-07-19	[Arcmed Group]	hunters	Link
2024-07-19	[Leech Lake Gaming]	cicada3301	Link
2024-07-15	[concorddirect.com]	lockbit3	Link
2024-07-15	[townandforest.co.uk]	lockbit3	Link
2024-07-17	[norton.k12.ma.us]	lockbit3	Link
2024-07-17	[energateinc.com]	lockbit3	Link
2024-07-17	[plantmachineworks.com]	lockbit3	Link
2024-07-17	[piedmonthoist.com]	lockbit3	Link
2024-07-17	[gptchb.org]	lockbit3	Link
2024-07-17	[assih.com]	lockbit3	Link
2024-07-18	[wattlerange.sa.gov.au]	lockbit3	Link
2024-07-18	[claycountyin.gov]	lockbit3	Link
2024-07-18	[iteam.gr]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-18	[albonanova.at]	lockbit3	Link
2024-07-18	[lothar-rapp.de]	lockbit3	Link
2024-07-18	[goldstarmetal.com]	lockbit3	Link
2024-07-18	[glsco.com]	lockbit3	Link
2024-07-18	[paysdelaloire.fr]	lockbit3	Link
2024-07-18	[troyareasd.org]	lockbit3	Link
2024-07-18	[barkingwell.gr]	lockbit3	Link
2024-07-18	[fbrlaw.com]	lockbit3	Link
2024-07-18	[customssupport.be]	lockbit3	Link
2024-07-18	[joliet86.org]	lockbit3	Link
2024-07-16	[www.glowfm.nl]	ransomhub	Link
2024-07-19	[Law Offices of the Public Defender - New Mexico]	rhysida	Link
2024-07-05	[Infomedika]	ransomhouse	Link
2024-07-17	[Next step healthcar]	qilin	Link
2024-07-18	[Northeast Rehabilitation Hospital Network]	hunters	Link
2024-07-18	[Seamon Whiteside]	hunters	Link
2024-07-18	[Santa Rosa]	hunters	Link
2024-07-18	[all-mode.com]	donutleaks	Link
2024-07-14	[www.erma-rtmo.it]	ransomhub	Link
2024-07-16	[metalfrio.com.br]	ransomhub	Link
2024-07-16	[www.newcastlewa.gov]	ransomhub	Link
2024-07-18	[pgd.pl]	ransomhub	Link
2024-07-17	[Modernauto]	blackbyte	Link
2024-07-17	[Modern Automotive Group]	blackbyte	Link
2024-07-17	[Gandara Center]	rhysida	Link
2024-07-17	[C???o???m]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-17	[Hayden Power Group]	play	Link
2024-07-17	[MIPS Technologies]	play	Link
2024-07-17	[ZSZAALEJI.cz]	qilin	Link
2024-07-17	[Eyal Baror the key official of the 8200 unit]	handala	Link
2024-07-17	[labline.it]	donutleaks	Link
2024-07-16	[www.hlbpr.com]	ransomhub	Link
2024-07-17	[isometrix.com]	cactus	Link
2024-07-06	[A.L.P. Lighting Components]	incransom	Link
2024-07-16	[VITALDENT]	madliberator	Link
2024-07-12	[BENICULTURALI.IT]	madliberator	Link
2024-07-12	[MONTERO & SEGURA]	madliberator	Link
2024-07-12	[crosswear.co.uk]	madliberator	Link
2024-07-12	[sacities.net]	madliberator	Link
2024-07-17	[zb.co.zw]	madliberator	Link
2024-07-17	[The Law Office of Omar O. Vargas, P.C.]	everest	Link
2024-07-17	[STUDIO NOTARILE BUCCI – OLMI]	everest	Link
2024-07-16	[GroupePRO-B]	cicada3301	Link
2024-07-16	[Greenheck]	meow	Link
2024-07-16	[CBIZ Inc]	meow	Link
2024-07-16	[Hewlett Packard Enterprise]	meow	Link
2024-07-16	[BCS Systems]	meow	Link
2024-07-16	[Guhring]	meow	Link
2024-07-16	[Odfjell Drilling]	meow	Link
2024-07-16	[Golan Christie Taglia]	meow	Link
2024-07-16	[First Commonwealth Federal Credit Union]	meow	Link
2024-07-07	[Djg Projects]	fog	Link
2024-07-04	[Verweij Elektrotechniek]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-04	[Alvin Independent School District]	fog	Link
2024-07-11	[West Allis-West Milwaukee School District]	fog	Link
2024-07-16	[German University of Technology in Oman]	fog	Link
2024-07-16	[ceopag.com.br / ceofood.com.br]	ransomhub	Link
2024-07-16	[[temporary] Warning for Eyal Baror]	handala	Link
2024-07-16	[www.benchinternational.com]	ransomhub	Link
2024-07-16	[www.cameronhodges.com]	ransomhub	Link
2024-07-16	[Braum's Inc]	hunters	Link
2024-07-16	[Lantronix Inc.]	hunters	Link
2024-07-16	[HOYA Corporation]	hunters	Link
2024-07-16	[Mainland Machinery]	dragonforce	Link
2024-07-16	[SBRPCA]	dragonforce	Link
2024-07-16	[verco.co.uk]	cactus	Link
2024-07-15	[Nuevatel]	dunghill	Link
2024-07-15	[Innovalve Bio Medical]	handala	Link
2024-07-09	[www.baiminstitute.org]	ransomhub	Link
2024-07-13	[integraservices]	mallox	Link
2024-07-14	[XENAPP-GLOBER]	mallox	Link
2024-07-15	[Gramercy Surgery Center]	everest	Link
2024-07-15	[posiplus.com]	blackbasta	Link
2024-07-15	[hpecds.com]	blackbasta	Link
2024-07-15	[Amino Transport]	akira	Link
2024-07-15	[Goede, DeBoest & Cross, PLLC.]	rhysida	Link
2024-07-15	[Sheba Medical Center]	handala	Link
2024-07-15	[usdermpartners.com]	blackbasta	Link
2024-07-15	[atos.com]	blackbasta	Link
2024-07-15	[Gibbs Hurley Chartered Accountants]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-15	[ComNet Communications]	hunters	Link
2024-07-15	[MS Ultrasonic Technology Group]	hunters	Link
2024-07-15	[RZO]	hunters	Link
2024-07-15	[thompsoncreek.com_wa]	blackbasta	Link
2024-07-15	[northernsafety.com_wa]	blackbasta	Link
2024-07-15	[upcli.com]	cloak	Link
2024-07-15	[greenlightbiosciences.com]	abyss	Link
2024-07-15	[valleylandtitleco.com - UPD]	donutleaks	Link
2024-07-14	[luzan5.com]	blackout	Link
2024-07-14	[BrownWinick]	rhysida	Link
2024-07-14	[Texas Alcohol & Drug Testing Service]	bianlian	Link
2024-07-13	[a-g.com - data publication 38gb (150K)]	blacksuit	Link
2024-07-13	[gbhs.org Publication 51gb]	blacksuit	Link
2024-07-13	[Kenya Urban Roads Authority]	hunters	Link
2024-07-13	[Carigali Hess Operating Company]	hunters	Link
2024-07-13	[gbhs.org 07/12 Publication 51gb]	blacksuit	Link
2024-07-01	[The Coffee Bean & Tea Leaf]	incransom	Link
2024-07-01	[State of Alabama - Alabama Department Of Education]	incransom	Link
2024-07-02	[ARISTA]	spacebears	Link
2024-07-12	[Preferred IT Group]	bianlian	Link
2024-07-08	[Wagner-Meinert]	ransomexx	Link
2024-07-12	[painproclinics.com]	ransomcortex	Link
2024-07-02	[www.zepter.de]	ransomhub	Link
2024-07-11	[www.riteaid.com]	ransomhub	Link
2024-07-03	[olympusgrp.com]	dispossessor	Link
2024-07-12	[www.donaanita.com]	ransomcortex	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-12	[perfeitaplastica.com.br]	ransomcortex	Link
2024-07-12	[www.respirarlondrina.com.br]	ransomcortex	Link
2024-07-11	[Hyperice]	play	Link
2024-07-11	[diligentusa.com]	embargo	Link
2024-07-11	[Image Microsystems]	blacksuit	Link
2024-07-11	[www.lynchaluminum.com]	ransomhub	Link
2024-07-11	[www.eurostrand.de]	ransomhub	Link
2024-07-11	[www.netavent.dk]	ransomhub	Link
2024-07-11	[Financoop]	akira	Link
2024-07-11	[Sigma]	akira	Link
2024-07-11	[Sonol (Gas Stations)]	handala	Link
2024-07-11	[www.bfcsolutions.com]	ransomhub	Link
2024-07-11	[Texas Electric Cooperatives]	play	Link
2024-07-11	[The 21st Century Energy Group]	play	Link
2024-07-11	[T P C I]	play	Link
2024-07-10	[City of Cedar Falls]	blacksuit	Link
2024-07-10	[P448]	akira	Link
2024-07-10	[Beowulfchain]	vanirgroup	Link
2024-07-10	[Qinao]	vanirgroup	Link
2024-07-10	[Athlon]	vanirgroup	Link
2024-07-10	[Usina Alta Mogiana S/A]	akira	Link
2024-07-09	[Inland Audio Visual]	akira	Link
2024-07-09	[Indika Energy]	hunters	Link
2024-07-08	[Excelsior Orthopaedics]	monti	Link
2024-07-09	[Heidmar]	akira	Link
2024-07-03	[REPLIGEN]	incransom	Link
2024-07-08	[Raffmetal Spa]	dragonforce	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-08	[Allied Industrial Group]	akira	Link
2024-07-08	[Esedra]	akira	Link
2024-07-08	[Federated Co-operatives]	akira	Link
2024-07-02	[Guhring USA]	incransom	Link
2024-07-06	[noab.nl]	lockbit3	Link
2024-07-07	[Strauss Brands]	medusa	Link
2024-07-07	[Harry Perkins Institute of medical research]	medusa	Link
2024-07-07	[Viasat]	medusa	Link
2024-07-07	[Olympus Group]	medusa	Link
2024-07-07	[MYC Media]	rhysida	Link
2024-07-06	[a-g.com 7/10/24 - data publication 38gb (150K)]	blacksuit	Link
2024-07-03	[baiminstitute.org]	ransomhub	Link
2024-07-05	[The Wacks Law Group]	qilin	Link
2024-07-05	[pomalca.com.pe]	qilin	Link
2024-07-05	[Center for Human Capital Innovation (centerforhci.org)]	incransom	Link
2024-07-05	[waupacacounty-wi.gov]	incransom	Link
2024-07-05	[waupaca.wi.us]	incransom	Link
2024-07-04	[ws-stahl.eu]	lockbit3	Link
2024-07-04	[homelandvinyl.com]	lockbit3	Link
2024-07-04	[eicher.in]	lockbit3	Link
2024-07-05	[National Health Laboratory Services]	blacksuit	Link
2024-07-04	[Un Museau]	spacebears	Link
2024-07-03	[Haylem]	spacebears	Link
2024-07-04	[Elyria Foundry]	play	Link
2024-07-04	[Texas Recycling]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-04	[INDA's]	play	Link
2024-07-04	[Innerspec Technologies]	play	Link
2024-07-04	[Prairie Athletic Club]	play	Link
2024-07-04	[Fareri Associates]	play	Link
2024-07-04	[Island Transportation Corp.]	bianlian	Link
2024-07-04	[Legend Properties, Inc.]	bianlian	Link
2024-07-04	[Transit Mutual Insurance Corporation]	bianlian	Link
2024-07-03	[hcri.edu]	ransomhub	Link
2024-07-04	[Coquitlam Concrete]	hunters	Link
2024-07-04	[Multisuns Communication]	hunters	Link
2024-07-04	[gerard-perrier.com]	embargo	Link
2024-07-04	[Abileneisd.org]	cloak	Link
2024-07-03	[sequelglobal.com]	darkvault	Link
2024-07-03	[Explomin]	akira	Link
2024-07-03	[Alimac]	akira	Link
2024-07-03	[badel1862.hr]	blackout	Link
2024-07-03	[ramservices.com]	underground	Link
2024-07-03	[foremedia.net]	darkvault	Link
2024-07-03	[www.swcs-inc.com]	ransomhub	Link
2024-07-03	[valleylandtitleco.com]	donutleaks	Link
2024-07-02	[merrymanhouse.org]	lockbit3	Link
2024-07-02	[fairfieldmemorial.org]	lockbit3	Link
2024-07-02	[www.daesangamerica.com]	ransomhub	Link
2024-07-02	[P1 Technologies]	akira	Link
2024-07-02	[Conexus Medstaff]	akira	Link
2024-07-02	[Salton]	akira	Link
2024-07-01	[www.sfmedical.de]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-07-02	[WheelerShip]	hunters	Link
2024-07-02	[Grand Rapids Gravel]	dragonforce	Link
2024-07-02	[Franciscan Friars of the Atonement]	dragonforce	Link
2024-07-02	[Elite Fitness]	dragonforce	Link
2024-07-02	[Gray & Adams]	dragonforce	Link
2024-07-02	[Vermont Panurgy]	dragonforce	Link
2024-07-01	[floridahealth.gov]	ransomhub	Link
2024-07-01	[www.nttdata.ro]	ransomhub	Link
2024-07-01	[Super Gardens]	dragonforce	Link
2024-07-01	[Hampden Veterinary Hospital]	dragonforce	Link
2024-07-01	[Indonesia Terkoneksi]	BrainCipher	Link
2024-07-01	[SYNERGY PEANUT]	akira	Link
2024-07-01	[Ethypharm]	underground	Link
2024-07-01	[latinusa.co.id]	lockbit3	Link
2024-07-01	[kbc-zagreb.hr]	lockbit3	Link
2024-07-01	[maxcess-logistics.com]	killsec	Link
2024-07-01	[Independent Education System]	handala	Link
2024-07-01	[Bartlett & Weigle Co. LPA.]	hunters	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.