Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240829

Inhaltsverzeichnis

1 Editorial **2**

2 Security-News **3**
2.1 Heise - Security-Alert . . . 3

3 Sicherheitslücken **4**
3.1 EPSS . . . 4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . 5
3.2 BSI - Warn- und Informationsdienst (WID) . . . 7
3.3 Sicherheitslücken Meldungen von Tenable . . . 11

4 Aktiv ausgenutzte Sicherheitslücken **13**
4.1 Exploits der letzten 5 Tage . . . 13
4.2 0-Days der letzten 5 Tage . . . 17

5 Die Hacks der Woche **18**
5.0.1 AI ist nicht bereit für Production (Indirekte Prompt Injection in der Slack AI) . . . 18

6 Cyberangriffe: (Aug) **19**

7 Ransomware-Erpressungen: (Aug) **20**

8 Quellen **35**
8.1 Quellenverzeichnis . . . 35

9 Impressum **36**

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

Hitachi Ops Center: Attacken auf Hitachi-Speicherinfrastruktur möglich

Hitachi Ops Center Common Services ist unter Linux verwundbar. Eine abgesicherte Version ist erschienen.

- Link

—

Ticketsystem OTRS: Angreifer können unverschlüsselte Passwörter einsehen

Die Entwickler des Open Ticket Request System haben mehrere Sicherheitslücken geschlossen.

- Link

—

Jetzt patchen! Netzwerksoftware Versa Director attackiert

Derzeit nutzen Angreifer eine Schwachstelle in der Virtualisierungs- und Serviceerstellungsplattform Versa Director aus.

- Link

—

Wordpress: 1 Million Webseiten nutzen verwundbares Plug-in WPML

Das Wordpress-Plug-in WPML kommt auf mehr als eine Million aktive Installationen. Jetzt wurde eine kritische Lücke darin gestopft.

- Link

—

Webbrowser: Weitere Lücke aktiv ausgenutzt, Adobe PDF-Viewer aktualisiert

Google meldet das Ausnutzen einer weiteren Lücke in freier Wildbahn. Die Updates von Edge schließen auch ein Leck im Adobe PDF Viewer.

- Link

—

Notfall-Update: Microsoft behebt riskante Sicherheitslücke in Edge

Google hat die Lücke im jüngsten Chrome-Update gepatcht, es gibt Hinweise auf aktive Exploits. Daher zieht Redmond nun nach.

- Link

—

Update verfügbar: IT-Sicherheitslösung IBM QRadar SIEM ist verwundbar

IBM hat mehrere Sicherheitslücken in verschiedenen Komponenten von QRadar SIEM geschlossen.

- Link

—

Bamboo, Confluence, Jira und Co.: Atlassian schließt hochriskante Lücken

Atlassian hat Updates für zahlreiche Produkte veröffentlicht. Sie schließen als hohes Risiko geltende Sicherheitslücken etwa in Bambo, Confluence und Jira.
- Link

—

Sicherheitsupdate: Attacken auf Sonicwall-Firewalls können Crash auslösen

Um Netzwerke von Unternehmen zu schützen, sollten Admins ihre Firewalls von Sonicwall zeitnah auf den aktuellen Stand bringen.
- Link

—

Hartkodierte Zugangsdaten gefährden Solarwinds Web Help Desk

Angreifer können unbefugt auf die Kundensupport-Software Web Help Desk von Solarwinds zugreifen und Daten manipulieren.
- 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-2023-6895	0.921160000	0.990060000	Link
CVE-2023-6553	0.921020000	0.990040000	Link
CVE-2023-6019	0.918710000	0.989820000	Link
CVE-2023-5360	0.902780000	0.988810000	Link
CVE-2023-52251	0.946410000	0.992910000	Link
CVE-2023-4966	0.971280000	0.998340000	Link
CVE-2023-49103	0.964030000	0.996070000	Link
CVE-2023-48795	0.965330000	0.996470000	Link
CVE-2023-47246	0.959760000	0.995190000	Link
CVE-2023-46805	0.934240000	0.991500000	Link
CVE-2023-46747	0.972900000	0.998930000	Link
CVE-2023-46604	0.964990000	0.996320000	Link
CVE-2023-4542	0.936770000	0.991700000	Link
CVE-2023-43208	0.972610000	0.998790000	Link
CVE-2023-43177	0.961750000	0.995560000	Link
CVE-2023-42793	0.970220000	0.997900000	Link
CVE-2023-41265	0.911110000	0.989340000	Link
CVE-2023-39143	0.940480000	0.992120000	Link
CVE-2023-38646	0.906950000	0.989060000	Link
CVE-2023-38205	0.953670000	0.994150000	Link
CVE-2023-38203	0.966410000	0.996750000	Link
CVE-2023-38146	0.920720000	0.990010000	Link
CVE-2023-38035	0.974690000	0.999720000	Link
CVE-2023-36845	0.966750000	0.996880000	Link
CVE-2023-3519	0.965910000	0.996610000	Link
CVE-2023-35082	0.967460000	0.997060000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.970450000	0.997980000	Link
CVE-2023-34993	0.973130000	0.999040000	Link
CVE-2023-34960	0.928290000	0.990840000	Link
CVE-2023-34634	0.925130000	0.990530000	Link
CVE-2023-34362	0.970450000	0.997980000	Link
CVE-2023-34039	0.952470000	0.993950000	Link
CVE-2023-3368	0.937150000	0.991740000	Link
CVE-2023-33246	0.967180000	0.996980000	Link
CVE-2023-32315	0.970220000	0.997900000	Link
CVE-2023-30625	0.953610000	0.994140000	Link
CVE-2023-30013	0.965950000	0.996620000	Link
CVE-2023-29300	0.969240000	0.997570000	Link
CVE-2023-29298	0.941540000	0.992260000	Link
CVE-2023-28432	0.911820000	0.989380000	Link
CVE-2023-28343	0.933130000	0.991400000	Link
CVE-2023-28121	0.919520000	0.989900000	Link
CVE-2023-27524	0.970600000	0.998040000	Link
CVE-2023-27372	0.973470000	0.999150000	Link
CVE-2023-27350	0.969720000	0.997730000	Link
CVE-2023-26469	0.951470000	0.993720000	Link
CVE-2023-26360	0.963510000	0.995920000	Link
CVE-2023-26035	0.969020000	0.997470000	Link
CVE-2023-25717	0.954250000	0.994250000	Link
CVE-2023-25194	0.967920000	0.997200000	Link
CVE-2023-2479	0.963960000	0.996040000	Link
CVE-2023-24489	0.973820000	0.999310000	Link
CVE-2023-23752	0.956380000	0.994650000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23333	0.962300000	0.995660000	Link
CVE-2023-22527	0.968780000	0.997420000	Link
CVE-2023-22518	0.965200000	0.996420000	Link
CVE-2023-22515	0.972340000	0.998650000	Link
CVE-2023-21839	0.955020000	0.994400000	Link
CVE-2023-21554	0.955880000	0.994560000	Link
CVE-2023-20887	0.970670000	0.998050000	Link
CVE-2023-1671	0.964660000	0.996210000	Link
CVE-2023-0669	0.969760000	0.997740000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 28 Aug 2024

[UPDATE] [hoch] Drupal: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Drupal ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- Link

—

Wed, 28 Aug 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, 28 Aug 2024

[UPDATE] [kritisch] Apache OFBiz: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 28 Aug 2024

[NEU] [hoch] Dell BIOS: Schwachstelle ermöglicht Codeausführung und Umgehung von Sicherheitsmaßnahmen

Ein lokaler Angreifer kann eine Schwachstelle in Dell BIOS ausnutzen, um beliebigen Programmcode auszuführen oder zur Umgehung von Sicherheitsmaßnahmen.

- Link

—

Wed, 28 Aug 2024

[NEU] [UNGEPATCHT] [hoch] D-LINK Router DIR-846W: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen im D-LINK Router DIR-846W ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Tue, 27 Aug 2024

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

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

- Link

—

Tue, 27 Aug 2024

[UPDATE] [kritisch] Microsoft Windows: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Windows, Microsoft Windows 10, Microsoft Windows 11, Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019 und Microsoft Windows Server 2022 ausnutzen, um beliebigen Programmcode auszuführen, beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 27 Aug 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen, UI-Spoofing zu betreiben, Sicherheitsmechanismen zu umgehen und andere nicht spezifizierte Angriffe durchzuführen.

- Link

—

Tue, 27 Aug 2024

[NEU] [hoch] Red Hat JBoss Enterprise Application Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat JBoss Enterprise Application Platform auf Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben, Dateien und Daten zu manipulieren oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Mon, 26 Aug 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

—

Mon, 26 Aug 2024

[NEU] [hoch] OTRS: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in OTRS ausnutzen, um einen Cross-Site-Scripting-Angriff zu starten oder vertrauliche Informationen offenzulegen.

- Link

—

Mon, 26 Aug 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Traffic Server ausnutzen, um einen Denial of Service Angriff durchzuführen oder Sicherheitsmaßnahmen zu umgehen.

- Link

—

Mon, 26 Aug 2024

[UPDATE] [hoch] fetchmail: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in fetchmail ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.

- Link

—

Mon, 26 Aug 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen, Daten zu manipulieren und den Benutzer zu täuschen.

- Link

—

Mon, 26 Aug 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

—

Mon, 26 Aug 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

—

Mon, 26 Aug 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

—

Mon, 26 Aug 2024

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

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

- Link

—

Fri, 23 Aug 2024

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- Link

—

Fri, 23 Aug 2024

[NEU] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um falsche Informationen

darzustellen und beliebigen Code auszuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 41 for SLE 15 SP2) (SUSE-SU-2024:3023-1)]	critical
8/28/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : openssl-3 (SUSE-SU-2024:3019-1)]	critical
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 41 for SLE 15 SP3) (SUSE-SU-2024:3041-1)]	critical
8/28/2024	[SUSE SLES12 Security Update : kernel (Live Patch 53 for SLE 12 SP5) (SUSE-SU-2024:3027-1)]	critical
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 35 for SLE 15 SP3) (SUSE-SU-2024:3030-1)]	critical
8/28/2024	[SUSE SLES12 Security Update : kernel (Live Patch 47 for SLE 12 SP5) (SUSE-SU-2024:3040-1)]	critical
8/28/2024	[SUSE SLES12 Security Update : kernel (Live Patch 49 for SLE 12 SP5) (SUSE-SU-2024:3014-1)]	critical
8/28/2024	[SUSE SLES12 Security Update : kernel (Live Patch 48 for SLE 12 SP5) (SUSE-SU-2024:3021-1)]	critical
8/28/2024	[SUSE SLES15 Security Update : keepalived (SUSE-SU-2024:3031-1)]	critical
8/28/2024	[SolarWinds Web Help Desk < 12.8.3 HF 2 HardCoded Credentials]	critical
8/28/2024	[Magento XXE (CVE-2024-34102)]	critical
8/28/2024	[CentOS 9 : openssl-3.2.2-4.el9]	critical

Datum	Schwachstelle	Bewertung
8/28/2024	[Slackware Linux 15.0 kcron Vulnerability (SSA:2024-240-01)]	high
8/28/2024	[Slackware Linux 15.0 plasma-workspace Vulnerability (SSA:2024-240-02)]	high
8/28/2024	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2024-076)]	high
8/28/2024	[Fedora 40 : dovecot (2024-e23e8a3f1e)]	high
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 44 for SLE 15 SP3) (SUSE-SU-2024:3039-1)]	high
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 47 for SLE 15 SP2) (SUSE-SU-2024:3044-1)]	high
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 46 for SLE 15 SP2) (SUSE-SU-2024:3043-1)]	high
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 43 for SLE 15 SP3) (SUSE-SU-2024:3048-1)]	high
8/28/2024	[SUSE SLES12 Security Update : kernel (Live Patch 54 for SLE 12 SP5) (SUSE-SU-2024:3037-1)]	high
8/28/2024	[Fedora 39 : dovecot (2024-ba5bb9f63a)]	high
8/28/2024	[SUSE SLES12 Security Update : kernel (Live Patch 56 for SLE 12 SP5) (SUSE-SU-2024:3015-1)]	high
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 0 for SLE 15 SP6) (SUSE-SU-2024:3032-1)]	high
8/28/2024	[SUSE SLES15 Security Update : kernel (Live Patch 42 for SLE 15 SP3) (SUSE-SU-2024:3034-1)]	high
8/28/2024	[ManageEngine ADAudit Plus < Build 8121 Multiple Vulnerabilities]	high
8/28/2024	[ManageEngine ADAudit Plus < Build 8000 Multiple Vulnerabilities]	high
8/28/2024	[RHEL 7 : bind (RHSA-2024:5930)]	high
8/28/2024	[ManageEngine OpManager RCE (CVE-2024-5466)]	high
8/28/2024	[Juniper Junos OS DoS (JSA82988)]	high

Datum	Schwachstelle	Bewertung
8/28/2024	[Atlassian Jira Service Management Data Center and Server 5.4.x < 5.4.25 / 5.12.x < 5.12.12 / 5.15.x < 5.17.1 DoS (JSDSERVER-15504)]	high
8/28/2024	[RHEL 8 : libvpx (RHSA-2024:5941)]	high
8/28/2024	[RHEL 9 : kernel (RHSA-2024:5928)]	high
8/28/2024	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel (Oracle) vulnerabilities (USN-6972-4)]	high
8/28/2024	[Google Chrome < 128.0.6613.114 Multiple Vulnerabilities]	high
8/28/2024	[Google Chrome < 128.0.6613.113 Multiple Vulnerabilities]	high
8/28/2024	[Google Chrome < 128.0.6613.113 Multiple Vulnerabilities]	high
8/28/2024	[Wireshark 4.0.x < 4.0.17 A Vulnerability]	high
8/28/2024	[Wireshark 4.0.x < 4.0.17 A Vulnerability (macOS)]	high
8/28/2024	[Wireshark 4.2.x < 4.2.7 A Vulnerability]	high
8/28/2024	[Wireshark 4.2.x < 4.2.7 A Vulnerability (macOS)]	high
8/28/2024	[CentOS 9 : python3.9-3.9.19-8.el9]	high
8/28/2024	[CentOS 9 : curl-7.76.1-31.el9]	high
8/28/2024	[CentOS 9 : kernel-5.14.0-503.el9]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 28 Aug 2024

WordPress LiteSpeed Cache 6.3.0.1 Privilege Escalation

WordPress LiteSpeed Cache versions 1.9 through 6.3.0.1 proof of concept privilege escalation exploit.

- Link

—

” “Wed, 28 Aug 2024

Microsoft Windows IPv6 Memory Corruption

This python script is a proof of concept exploit that demonstrates a IPv6 related memory corruption

in Microsoft Windows.

- Link

—

” “Wed, 28 Aug 2024

WordPress GiveWP Donation / Fundraising Platform 3.14.1 File Deletion / Command Execution

WordPress GiveWP Donation and Fundraising Platform plugins versions 3.14.1 and below suffer from file deletion and remote command execution vulnerabilities.

- Link

—

” “Wed, 28 Aug 2024

Qualcomm KGSL Mapping Issue

Qualcomm KGSL has an issue where reclaimed / in-reclaim objects can still be mapped into VBOs.

- Link

—

” “Wed, 28 Aug 2024

MSMS-PHP 1.0 Insecure Settings

MSMS-PHP version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 28 Aug 2024

Mount Carmel School 6.4.1 Insecure Settings

Mount Carmel School version 6.4.1 suffers from an ignored default credential vulnerability.

- Link

—

” “Wed, 28 Aug 2024

Laundry Management System 1.0 Remote File Inclusion

Laundry Management System version 1.0 suffers from a remote file inclusion vulnerability.

- Link

—

” “Wed, 28 Aug 2024

File Management System 1.0 Arbitrary File Upload

File Management System version 1.0 suffers from an arbitrary file upload vulnerability.

- Link

—

” “Wed, 28 Aug 2024

SPIP 4.2.2 Code Execution

SPIP version 4.2.2 suffers from a code execution vulnerability.

- Link

—

” “Tue, 27 Aug 2024

Linux lock_get_status() Use-After-Free

An LSM can prevent the fcntl/close race cleanup path in fcntl_setlk() from working, leading to use-after-free read in lock_get_status() when reading /proc/locks.

- Link

—

” “Tue, 27 Aug 2024

PowerVR DevmemIntChangeSparse2() Use-After-Free

PowerVR suffers from a use-after-free vulnerability in DevmemIntChangeSparse2() on a PMRGetUID() call.

- Link

—

” “Tue, 27 Aug 2024

miniProxy 1.0.0 Remote File Inclusion

miniProxy version 1.0.0 suffers from a remote file inclusion vulnerability.

- Link

—

” “Tue, 27 Aug 2024

Medicine Tracker System 1.0 Insecure Settings

Medicine Tracker System version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 27 Aug 2024

Medical Hub Directory Site 1.0 Insecure Settings

Medical Hub Directory Site version 1.0 suffers from an ignored default credential vulnerability.

- Link

—

” “Tue, 27 Aug 2024

Medical Center Portal 1.0 SQL Injection

Medical Center Portal version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 27 Aug 2024

Marc@TMS CMS 1.0 SQL Injection

Marc@TMS CMS version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 27 Aug 2024

Lodging Reservation Management System 1.0 Insecure Settings

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

- Link

—

” “Tue, 27 Aug 2024

Login System Project 1.0 SQL Injection

Login System Project version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- Link

—

” “Tue, 27 Aug 2024

Loan Management System 1.0 Remote File Inclusion

Loan Management System version 1.0 suffers from a remote file inclusion vulnerability.

- Link

—

” “Mon, 26 Aug 2024

Invesalius 3.1 Remote Code Execution

Invesalius versions 3.1.99991 through 3.1.99998 suffer from a remote code execution vulnerability. The exploitation steps of this vulnerability involve the use of a specifically crafted DICOM file which, once imported inside the victim’s client application, allows an attacker to gain remote code execution.

- Link

—

” “Mon, 26 Aug 2024

Calibre Web 0.6.21 Cross Site Scripting

Calibre Web version 0.6.21 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 26 Aug 2024

Helpdeskz 2.0.2 Cross Site Scripting

Helpdeskz version 2.0.2 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Mon, 26 Aug 2024

SPIP 4.2.11 Code Execution

SPIP version 4.2.11 suffers from a code execution vulnerability.
- Link
—
” “Mon, 26 Aug 2024
Loan Management System 1.0 SQL Injection
Loan Management System version 1.0 suffers from a remote SQL injection vulnerability that allows for authentication bypass.
- Link
—
” “Mon, 26 Aug 2024
Jobs Finder System 1.0 Cross Site Scripting
Jobs Finder System version 1.0 suffers from a cross site scripting vulnerability.
- Link
—
”

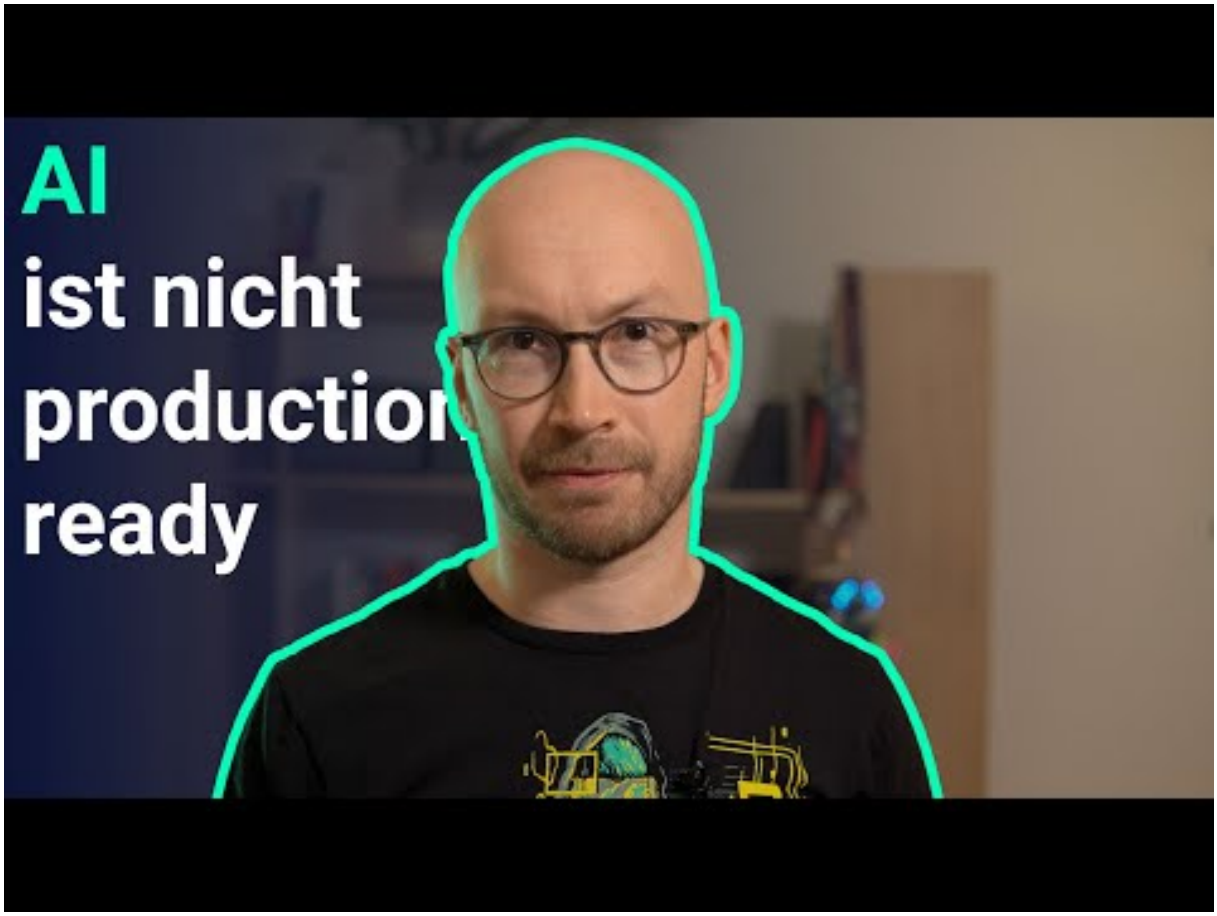
4.2 0-Days der letzten 5 Tage

“Tue, 27 Aug 2024
ZDI-24-1182: Linux Kernel Netfilter Conntrack Type Confusion Information Disclosure Vulnerability
- Link
—
”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 AI ist nicht bereit für Production (Indirekte Prompt Injection in der Slack AI)



Zum Youtube Video

6 Cyberangriffe: (Aug)

Datum	Opfer	Land	Information
2024-08-27	Portal do Governo do Estado de Alagoas	[BRA]	Link
2024-08-27	Direct Signalétique	[FRA]	Link
2024-08-25	Arntz Optibelt	[DEU]	Link
2024-08-25	La Cité de la BD d'Angoulême	[FRA]	Link
2024-08-24	Aéroport international Seattle-Tacoma	[USA]	Link
2024-08-24	Timişoara	[ROU]	Link
2024-08-24	Zeop	[FRA]	Link
2024-08-21	Groupe Cirano	[REU]	Link
2024-08-21	Halliburton	[USA]	Link
2024-08-21	Postnord	[SWE]	Link
2024-08-21	Dick's Sporting Goods, Inc.	[USA]	Link
2024-08-19	BVI Electricity Corporation (BVIEC)	[VGB]	Link
2024-08-18	Lagoon	[NCL]	Link
2024-08-18	Ponta Grossa	[BRA]	Link
2024-08-18	Pittsburg	[USA]	Link
2024-08-18	Banham Poultry	[GBR]	Link
2024-08-17	Bella Vista	[USA]	Link
2024-08-17	Microchip Technology Incorporated	[USA]	Link
2024-08-17	Octave	[FRA]	Link
2024-08-16	Contarina	[ITA]	Link
2024-08-16	Shoshone-Bannock Tribes	[USA]	Link
2024-08-15	Canvey Infant School	[GBR]	Link
2024-08-15	Cucamonga Valley Water District	[USA]	Link
2024-08-14	Flint	[USA]	Link
2024-08-14	NWO (Organisation néerlandaise pour la recherche scientifique)	[NLD]	Link

Datum	Opfer	Land	Information
2024-08-13	District scolaire indépendant de Gadsden	[USA]	Link
2024-08-13	IPNext	[ARG]	Link
2024-08-12	Benson, Kearley & Associates Insurance Brokers Ltd.	[CAN]	Link
2024-08-11	Université Paris-Saclay	[FRA]	Link
2024-08-11	AutoCanada	[CAN]	Link
2024-08-11	Itu	[BRA]	Link
2024-08-10	2Park	[NLD]	Link
2024-08-09	Quálitas	[MEX]	Link
2024-08-09	Schlatter Industries AG	[CHE]	Link
2024-08-08	Ohio School Boards Association (OSBA)	[USA]	Link
2024-08-08	Evolution Mining	[AUS]	Link
2024-08-07	Killeen	[USA]	Link
2024-08-06	Nilörn	[SWE]	Link
2024-08-06	Sumter County Sheriff's Office	[USA]	Link
2024-08-05	La ville de North Miami	[USA]	Link
2024-08-05	McLaren Health Care	[USA]	Link
2024-08-04	RMN-Grand Palais	[FRA]	Link
2024-08-04	Regent Caravans	[AUS]	Link
2024-08-03	Xtrim	[ECU]	Link
2024-08-02	Ihecs	[BEL]	Link

7 Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-29	[Appletec Ltd]	handala	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-28	[christen-sanitaer.ch]	cicada3301	Link
2024-08-28	[Bayou DeSiard Country Club - Monroe, LA]	cicada3301	Link
2024-08-26	[rainierarms.com]	ransomhub	Link
2024-08-28	[Epi Breads]	play	Link
2024-08-28	[Software Engineering Associates]	play	Link
2024-08-28	[GDB International]	play	Link
2024-08-28	[ABC Parts International]	play	Link
2024-08-28	[Universal Pure]	play	Link
2024-08-28	[Omicron Granite & Tile]	play	Link
2024-08-28	[Clabots]	play	Link
2024-08-29	[rmn.fr]	BrainCipher	Link
2024-08-28	[tjs.com]	killsec	Link
2024-08-28	[ghanare.com]	BrainCipher	Link
2024-08-28	[JM Thompson]	qilin	Link
2024-08-28	[medisetter.com]	killsec	Link
2024-08-28	[agra-services.be]	killsec	Link
2024-08-28	[Atwood & Cherny, P.C.]	bianlian	Link
2024-08-28	[Fish Nelson & Holden]	bianlian	Link
2024-08-28	[M.Royo & KlockMetal]	bianlian	Link
2024-08-28	[Scott Pharma Solutions]	bianlian	Link
2024-08-28	[freshairefranchise.com]	darkvault	Link
2024-08-28	[Diamcad]	meow	Link
2024-08-21	[tcn.local]	lynx	Link
2024-08-28	[mykukun.com]	killsec	Link
2024-08-28	[comtruck.ca]	abyss	Link
2024-08-07	[codacinc.org]	qilin	Link
2024-08-28	[Woden]	meow	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-28	[Y. Shilat Management Services Ltd]	meow	Link
2024-08-28	[Success Microfinance Bank]	meow	Link
2024-08-21	[KidKraft]	lynx	Link
2024-08-28	[Rinehart Butler Hodge Moss & Bryant]	hunters	Link
2024-08-27	[dpfza.gov.dj]	ransomhub	Link
2024-08-27	[www.polycohealthline.com]	ransomhub	Link
2024-08-27	[www.chwa.com.tw]	ransomhub	Link
2024-08-27	[WT Gruber Steuerberatung GmbH]	meow	Link
2024-08-27	[Finlogic S.p.A]	meow	Link
2024-08-27	[Academy of Model Aeronautics]	blacksuit	Link
2024-08-19	[Mason City Recycling Center]	qilin	Link
2024-08-27	[Barkal Food Industries]	meow	Link
2024-08-27	[Modulkit]	meow	Link
2024-08-27	[Artesanía Chopo]	meow	Link
2024-08-27	[Crowe]	hunters	Link
2024-08-27	[securityinstrument.com]	cactus	Link
2024-08-26	[Microchip Technology]	play	Link
2024-08-26	[Precom]	play	Link
2024-08-26	[All Parks Insurance]	meow	Link
2024-08-26	[Vans Lumber and Custom Builders]	meow	Link
2024-08-26	[Optimize EGS]	meow	Link
2024-08-26	[Complete Payroll Solutions]	meow	Link
2024-08-26	[South American Tours]	meow	Link
2024-08-26	[www.smarterp.com]	ransomhub	Link
2024-08-26	[htsusa.com]	ransomhub	Link
2024-08-26	[www.spie-tec.de]	ransomhub	Link
2024-08-26	[Brookshire Dental - Hospitals & Clinics]	qilin	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-16	[MacEwen Petroleum]	lynx	Link
2024-08-26	[pocketrisk.com]	darkvault	Link
2024-08-26	[widex.com]	blacksuit	Link
2024-08-26	[Blue Maven Group]	monti	Link
2024-08-26	[NewsBank]	rhysida	Link
2024-08-26	[US Marshals Service]	hunters	Link
2024-08-26	[onedayonly.co.za]	killsec	Link
2024-08-26	[Affordable Tools]	rhysida	Link
2024-08-25	[prasarana.com.my]	ransomhub	Link
2024-08-19	[Penn Veterinary Supply INC]	qilin	Link
2024-08-21	[Meli (BCYF & Bethany)]	qilin	Link
2024-08-25	[dt-technologies]	qilin	Link
2024-08-26	[autonomous.ai]	killsec	Link
2024-08-25	[Sable International]	bianlian	Link
2024-08-18	[The University and College Union]	incransom	Link
2024-08-25	[EPS Tech R&D]	handala	Link
2024-08-24	[nwcsb.com]	blacksuit	Link
2024-08-23	[Myelec Electrical]	lynx	Link
2024-08-24	[www.curvc.com]	ElDorado	Link
2024-08-24	[Eagle Safety Eyewear]	ElDorado	Link
2024-08-18	[Wallace Construction Specialties (wcs.local))]	lynx	Link
2024-08-18	[Bay Sales (cog.local)]	lynx	Link
2024-08-18	[PBS group]	lynx	Link
2024-08-18	[Health Quality Council]	incransom	Link
2024-08-24	[HBGJEWISHCOMMUN]	helldown	Link
2024-08-24	[ingotbrokers.com]	darkvault	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-24	[Hofmann Malerei AG]	cicada3301	Link
2024-08-24	[Studio Legale Associato Isolabella]	bianlian	Link
2024-08-22	[HL Lawson & Sons]	incransom	Link
2024-08-23	[terralogs.com.br]	killsec	Link
2024-08-23	[Chama Gaucha]	cicada3301	Link
2024-08-23	[idahopacific.com]	abyss	Link
2024-08-23	[barryavenueplating]	helldown	Link
2024-08-23	[rsk-immobilien]	helldown	Link
2024-08-23	[Crimson Interactive]	hunters	Link
2024-08-23	[www.seaeng.com]	dAn0n	Link
2024-08-23	[Stjamesplace.org]	cloak	Link
2024-08-23	[Saeilo]	metaencryptor	Link
2024-08-22	[schoolrush.com]	killsec	Link
2024-08-22	[Life University]	metaencryptor	Link
2024-08-22	[Sherwood Stainless & Aluminium]	dragonforce	Link
2024-08-22	[Igloo Cellulose]	dragonforce	Link
2024-08-22	[Raifalsa-Alelor]	dragonforce	Link
2024-08-22	[Deane Roofing and Cladding]	dragonforce	Link
2024-08-22	[instadriver.co]	killsec	Link
2024-08-22	[cincinnatipainphysicians]	helldown	Link
2024-08-22	[Don’t Waste Group]	incransom	Link
2024-08-22	[Kronick Moskovitz Tiedemann & Girard]	rhysida	Link
2024-08-22	[UFCW Local 135]	cicada3301	Link
2024-08-22	[EBA Ernest Bland Associates]	cicada3301	Link
2024-08-22	[level.game]	killsec	Link
2024-08-22	[antaeustravel.com]	blackout	Link
2024-08-22	[rylandpeters.com]	apt73	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-22	[saudi arabia(general secretariat of the military service council)]	ransomhub	Link
2024-08-22	[Engedi]	rhysida	Link
2024-08-22	[EPS Tech confidential source code (military)]	handala	Link
2024-08-16	[policiaauxiliarcusaem.com.mx]	lockbit3	Link
2024-08-14	[Larc]	incransom	Link
2024-08-22	[kbosecurity.co.uk]	helldown	Link
2024-08-22	[khonaysser.com]	helldown	Link
2024-08-21	[beinlaw.co.il - Prof. Bein & Co.]	BrainCipher	Link
2024-08-21	[The SMS Group]	play	Link
2024-08-21	[Grid Subject Matter Experts]	play	Link
2024-08-21	[Quilvest Capital Partners]	play	Link
2024-08-21	[Armour Coatings]	play	Link
2024-08-21	[RCG]	play	Link
2024-08-21	[Policy Administration Solutions]	play	Link
2024-08-21	[Dunlop Aircraft Tyres]	cloak	Link
2024-08-21	[Vibo.dk]	cloak	Link
2024-08-21	[Hvb-ingenieure.de]	cloak	Link
2024-08-21	[Westermans.com]	cloak	Link
2024-08-21	[Jinny Corporation]	akira	Link
2024-08-21	[BARRYAVEPLATING]	helldown	Link
2024-08-21	[RSK-IMMOBILIEN]	helldown	Link
2024-08-20	[capitalfund1.com]	ransomhub	Link
2024-08-21	[www.pindrophearing.co.uk]	apt73	Link
2024-08-21	[www.banhampoultry.co.uk]	ransomhub	Link
2024-08-21	[kidkraft.com]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-21	[Luigi Convertini]	ciphbit	Link
2024-08-21	[Findel]	cicada3301	Link
2024-08-21	[HOERBIGER Holding]	akira	Link
2024-08-21	[Olympus Financial]	rhysida	Link
2024-08-21	[spvmhc.org]	abyss	Link
2024-08-21	[Burns Industrial Equipment]	meow	Link
2024-08-21	[globacap.com]	apt73	Link
2024-08-20	[Codival]	spacebears	Link
2024-08-21	[jpoint.in]	killsec	Link
2024-08-20	[inlighten.net]	ransomhub	Link
2024-08-20	[blowerdempsay.com]	ransomhub	Link
2024-08-20	[ATP]	helldown	Link
2024-08-20	[Rushlift (lks.net)]	lynx	Link
2024-08-20	[North Georgia Brick]	akira	Link
2024-08-20	[Akkanat Holding]	hunters	Link
2024-08-19	[Percento Technologies Internationa]	medusa	Link
2024-08-19	[OSG.COM]	ransomhub	Link
2024-08-14	[imobesidade.com.br]	ransomhub	Link
2024-08-19	[Waynesboro Nurseries]	rhysida	Link
2024-08-19	[The Transit Authority of Northern Kentucky (TANK)]	akira	Link
2024-08-19	[Khonaysser]	helldown	Link
2024-08-11	[Jangho Group]	ransomhouse	Link
2024-08-19	[Certified Transmission]	meow	Link
2024-08-19	[Bandier]	blacksuit	Link
2024-08-18	[ccsdschools.com]	ransomhub	Link
2024-08-19	[Ferraro Group]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-18	[kbo]	helldown	Link
2024-08-18	[Mohawk Valley Cardiology PC]	bianlian	Link
2024-08-18	[PBC Companies]	bianlian	Link
2024-08-17	[Yang Enterprises]	dragonforce	Link
2024-08-17	[Carver Companies]	dragonforce	Link
2024-08-17	[J&J Network Engineering]	dragonforce	Link
2024-08-18	[PER4MANCE]	dragonforce	Link
2024-08-18	[SMK Ingenieurbüro]	dragonforce	Link
2024-08-18	[Cosmetic Dental Group]	trinity	Link
2024-08-17	[TELECO]	stormous	Link
2024-08-17	[peoplewell.com]	darkvault	Link
2024-08-17	[aerworldwide.com]	lockbit3	Link
2024-08-17	[awsag.com]	madliberator	Link
2024-08-17	[www.albynhousing.org.uk]	ransomhub	Link
2024-08-17	[www.lennartsfors.com]	ransomhub	Link
2024-08-17	[www.allanmcneill.co.nz]	ransomhub	Link
2024-08-17	[www.martinswood.herts.sch.uk]	ransomhub	Link
2024-08-17	[www.gmchc.org]	ransomhub	Link
2024-08-17	[www.regentcaravans.com.au]	ransomhub	Link
2024-08-17	[www.netconfig.co.za]	ransomhub	Link
2024-08-17	[www.manotherm.ie]	ransomhub	Link
2024-08-17	[tiendasmacuto.com]	BrainCipher	Link
2024-08-15	[nrcollecties.nl]	ransomhub	Link
2024-08-17	[zyxel]	helldown	Link
2024-08-10	[www.wmwmeyer.com]	ransomhub	Link
2024-08-16	[www.vinakom.com]	ransomhub	Link
2024-08-16	[Keios Development Consulting]	ciphbit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-16	[Lennartsfors AB]	meow	Link
2024-08-16	[Rostance Edwards]	meow	Link
2024-08-16	[SuperDrob S.A.]	hunters	Link
2024-08-16	[Sterling Rope]	rhysida	Link
2024-08-16	[www.patelco.org]	ransomhub	Link
2024-08-14	[ljglaw.com]	ransomhub	Link
2024-08-16	[Hiesmayr Haustechnik]	qilin	Link
2024-08-15	[www.aaconsultinc.com]	ransomhub	Link
2024-08-16	[promises2kids.org]	qilin	Link
2024-08-16	[BTS Biogas]	hunters	Link
2024-08-15	[www.isnart.it]	ransomhub	Link
2024-08-15	[www.atwoodcherny.com]	ransomhub	Link
2024-08-13	[Mill Creek Lumber]	play	Link
2024-08-14	[Patterson Health Center]	qilin	Link
2024-08-15	[www.prinsotel.com]	qilin	Link
2024-08-15	[Seaway Manufacturing Corp.]	fog	Link
2024-08-15	[FD S.R.L]	ciphbit	Link
2024-08-15	[The Pyle Group]	medusa	Link
2024-08-15	[Zydus Pharmaceuticals]	meow	Link
2024-08-15	[EPS Tech Ltd]	handala	Link
2024-08-15	[MBS Radio]	metaencryptor	Link
2024-08-15	[Liberty Resources]	rhysida	Link
2024-08-15	[megatravel.com.mx]	darkvault	Link
2024-08-14	[startaxi.com]	killsec	Link
2024-08-14	[Boni]	akira	Link
2024-08-14	[The Washington Times]	rhysida	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-12	[Benson Kearley IFG - Insurance Brokers & Financial Advisors]	bianlian	Link
2024-08-14	[Texas Centers for Infectious Disease Associates]	bianlian	Link
2024-08-14	[Thompson Davis & Co]	bianlian	Link
2024-08-14	[police.praca.gov.pl]	ransomhub	Link
2024-08-14	[mmtransport.com]	dAn0n	Link
2024-08-14	[Riley Pope & Laney]	cicada3301	Link
2024-08-13	[hugwi]	helldown	Link
2024-08-13	[Forrec]	blacksuit	Link
2024-08-13	[American Contract Systems]	meow	Link
2024-08-13	[Element Food Solutions]	meow	Link
2024-08-13	[Aerotech Solutions]	meow	Link
2024-08-13	[E-Z UP]	meow	Link
2024-08-13	[Safefood]	meow	Link
2024-08-13	[Gaston Fence]	meow	Link
2024-08-13	[Parker Development Company]	play	Link
2024-08-13	[Air International Thermal Systems]	play	Link
2024-08-13	[Adina Design]	play	Link
2024-08-13	[CinemaTech]	play	Link
2024-08-13	[Erie Meats]	play	Link
2024-08-13	[M??? ????k ??????]	play	Link
2024-08-13	[SCHLATTNER]	helldown	Link
2024-08-13	[deganis]	helldown	Link
2024-08-13	[The White Center Community Development Association]	rhysida	Link
2024-08-13	[lenmed.co.za]	darkvault	Link
2024-08-13	[gpf.org.za]	darkvault	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-13	[Banner and Associates]	trinity	Link
2024-08-13	[Southwest Family Medicine Associates]	bianlian	Link
2024-08-13	[glazkov.co.il]	darkvault	Link
2024-08-05	[XPERT Business Solutions GmbH]	helldown	Link
2024-08-05	[MyFreightWorld]	helldown	Link
2024-08-09	[cbmm]	helldown	Link
2024-08-10	[AZIENDA TRASPORTI PUBBLICI S.P.A.]	helldown	Link
2024-08-11	[briju]	helldown	Link
2024-08-11	[vindix]	helldown	Link
2024-08-11	[Albatros]	helldown	Link
2024-08-12	[NetOne]	hunters	Link
2024-08-12	[fabamaq.com]	BrainCipher	Link
2024-08-12	[cyceron.fr]	BrainCipher	Link
2024-08-12	[bedford.k12.oh.us]	ransomhub	Link
2024-08-12	[Warwick Hotels and Resorts]	lynx	Link
2024-08-12	[VVS-Eksperten]	cicada3301	Link
2024-08-12	[Brookshire Dental]	qilin	Link
2024-08-07	[Alvan Blanch Development]	lynx	Link
2024-08-11	[parkerdevco.com]	dispossessor	Link
2024-08-11	[naturalcuriosities.com]	ransomhub	Link
2024-08-11	[TelPro]	play	Link
2024-08-11	[Jeffersoncountyclerk.org]	ransomhub	Link
2024-08-11	[Amco Metal Industrial Corporation]	qilin	Link
2024-08-11	[brockington.leisc.sch.uk]	lockbit3	Link
2024-08-11	[Moser Wealth Advisors]	rhysida	Link
2024-08-09	[alliuminteriors.co.nz]	ransomhub	Link
2024-08-11	[robertshvac.com]	abyss	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-11	[dmmerch.com]	lockbit3	Link
2024-08-11	[luisoliveras.com]	lockbit3	Link
2024-08-11	[legacycpas.com]	lockbit3	Link
2024-08-11	[allweatheraa.com]	lockbit3	Link
2024-08-11	[soprema.com]	lockbit3	Link
2024-08-11	[exol-lubricants.com]	lockbit3	Link
2024-08-11	[fremontschools.net]	lockbit3	Link
2024-08-11	[acdcexpress.com]	lockbit3	Link
2024-08-11	[clinicatezza.com.pe]	lockbit3	Link
2024-08-11	[divaris.com]	lockbit3	Link
2024-08-11	[sullivansteelservice.com]	lockbit3	Link
2024-08-11	[johnllowery.com]	lockbit3	Link
2024-08-11	[qespavements.com]	lockbit3	Link
2024-08-11	[emanic.net]	lockbit3	Link
2024-08-11	[Hanon Systems]	hunters	Link
2024-08-10	[kronospublic.com]	lockbit3	Link
2024-08-10	[Brontoo Technology Solutions]	ransomexx	Link
2024-08-07	[Cydcor]	dragonforce	Link
2024-08-09	[Credible Group]	play	Link
2024-08-09	[Nilorngruppen AB]	play	Link
2024-08-09	[www.arkworkplacerisk.co.uk]	alphalocker	Link
2024-08-09	[Anniversary Holding Company]	bianlian	Link
2024-08-09	[GCA Global Cargo Alliance]	bianlian	Link
2024-08-09	[Majestic Metals]	bianlian	Link
2024-08-09	[dhcgrp.com]	ransomhub	Link
2024-08-05	[Boombah Inc.]	incransom	Link
2024-08-09	[www.dunnsolutions.com]	dAn0n	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-09	[Sumter County Sheriff]	rhysida	Link
2024-08-06	[pierrediamonds.com.au]	ransomhub	Link
2024-08-08	[golfoy.com]	ransomhub	Link
2024-08-08	[inv-dar.com]	ransomhub	Link
2024-08-08	[icarasia.com]	killsec	Link
2024-08-08	[rationalenterprise.com]	ransomhub	Link
2024-08-02	[modernceramics.com]	ransomhub	Link
2024-08-08	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-08	[tibaitservices.com]	cactus	Link
2024-08-08	[mihlfeld.com]	cactus	Link
2024-08-08	[Horizon View Medical Center]	everest	Link
2024-08-08	[comoferta.com]	darkvault	Link
2024-08-08	[NIDEC CORPORATION]	everest	Link
2024-08-08	[mercadomineiro.com.br]	darkvault	Link
2024-08-07	[hudsoncivil.com.au]	ransomhub	Link
2024-08-07	[www.jgsummit.com.ph]	ransomhub	Link
2024-08-07	[Bayhealth Hospital]	rhysida	Link
2024-08-07	[amplicon.com]	ransomhub	Link
2024-08-06	[infotexim.pe]	ransomhub	Link
2024-08-07	[suandco.com]	madliberator	Link
2024-08-07	[Anderson Oil & Gas]	hunters	Link
2024-08-07	[bonatra.com]	killsec	Link
2024-08-07	[FatBoy Cellular]	meow	Link
2024-08-07	[KLA]	meow	Link
2024-08-07	[HUD User]	meow	Link
2024-08-06	[msprocuradores.es]	madliberator	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-06	[www.carri.com]	alphalocker	Link
2024-08-06	[www.consorzioinnova.it]	alphalocker	Link
2024-08-06	[goftac.com/ firsttx.com First Texas Alliance Corp (FTAC)]	alphalocker	Link
2024-08-06	[biw-burger.de]	alphalocker	Link
2024-08-06	[www.sobha.com]	ransomhub	Link
2024-08-06	[Alternate Energy]	play	Link
2024-08-06	[True Blue Environmental]	play	Link
2024-08-06	[Granit Design]	play	Link
2024-08-06	[KinetX]	play	Link
2024-08-06	[Omni Family Health]	hunters	Link
2024-08-06	[IOI Corporation Berhad]	fog	Link
2024-08-06	[Ziba Design]	fog	Link
2024-08-06	[Casco Antiguo]	hunters	Link
2024-08-06	[Fractalia Group]	hunters	Link
2024-08-06	[Banx Systems]	meow	Link
2024-08-05	[Silipos]	cicada3301	Link
2024-08-04	[kierlcpa.com]	lockbit3	Link
2024-08-05	[Square One Coating Systems]	cicada3301	Link
2024-08-05	[Hi-P International]	fog	Link
2024-08-05	[Zon Beachside zonbeachside.com]	dispossessor	Link
2024-08-05	[HP Distribution]	incransom	Link
2024-08-05	[exco-solutions.com]	cactus	Link
2024-08-05	[Maryville Academy]	rhysida	Link
2024-08-04	[notariusze.waw.pl]	killsec	Link
2024-08-04	[Ranney School]	rhysida	Link
2024-08-03	[nursing.com]	ransomexx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-03	[Bettis Asphalt]	blacksuit	Link
2024-08-03	[fcl.crs]	lockbit3	Link
2024-08-03	[CPA Tax Solutions]	meow	Link
2024-08-03	[LRN]	hunters	Link
2024-08-03	[aikenhousing.org]	blacksuit	Link
2024-08-02	[David E Shambach Architect]	dragonforce	Link
2024-08-02	[Hayes Beer Distributing]	dragonforce	Link
2024-08-02	[Jangho Group]	hunters	Link
2024-08-02	[Khandelwal Laboratories Pvt]	hunters	Link
2024-08-02	[retaildatallc.com]	ransomhub	Link
2024-08-02	[WPG Holdings]	meow	Link
2024-08-02	[National Beverage]	meow	Link
2024-08-02	[PeoplesHR]	meow	Link
2024-08-02	[Dometic Group]	meow	Link
2024-08-02	[Remitano]	meow	Link
2024-08-02	[Premier Equities]	meow	Link
2024-08-01	[Kemlon Products & Development Co Inc]	spacebears	Link
2024-08-02	[q-cells.de]	abyss	Link
2024-08-02	[coinbv.nl]	madliberator	Link
2024-08-01	[Valley Bulk]	cicada3301	Link
2024-08-01	[ENEA Italy]	hunters	Link
2024-08-01	[mcdowallaffleck.com.au]	ransomhub	Link
2024-08-01	[effinghamschools.com]	ransomhub	Link
2024-08-01	[warrendale-wagyu.co.uk]	darkvault	Link
2024-08-01	[Adorna & Guzman Dentistry]	monti	Link
2024-08-01	[Camp Susque]	medusa	Link
2024-08-01	[Ali Gohar]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-08-01	[acsi.org]	blacksuit	Link
2024-08-01	[County Linen UK]	dispossessor	Link
2024-08-01	[TNT Materials tnt-materials.com/]	dispossessor	Link
2024-08-01	[Peñoles]	akira	Link
2024-08-01	[dahlvalve.com]	cactus	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.